DATA PRIVACY IN THE FIRE SERVICE: UNDERSTANDING THE POLICY ENVIRONMENT, FIREFIGHTER PREFERENCES, AND LEADERSHIP PERSPECTIVES

by
Rachel Jamie Michi Topazian

A dissertation submitted to Johns Hopkins University in conformity with the requirements for the degree of Doctor of Philosophy

Baltimore, Maryland
April 2024

Abstract

Objective: Firefighters experience high rates of occupational injury and fatality while serving their communities. Despite growing interest in using health and safety data to understand and prevent injuries, little is known about the policies governing such data or firefighter or leadership perspectives on data privacy. This dissertation unpacks the policies governing firefighter occupational health and safety data in Maryland and Virginia and fire service stakeholders' views towards current and future data practices.

Methods: Manuscript One leveraged legal research methods to identify and analyze federal, Maryland, and Virginia laws and regulations, and local union contracts. Manuscripts Two and Three used interviews and focus groups to assess the views of firefighters and fire department leaders in Maryland and Virginia, as well as national-level leaders.

Results: There were few laws and regulations directly related to occupational health and safety data privacy; of the 20 laws and regulations we identified, federal policies were most comprehensive in addressing data privacy. 11 union contracts varied significantly, with some limiting data access and others authorizing surveillance. 65 participants across 35 interviews and 4 focus groups described similar current data collection practices. Firefighters had few concerns about current practices while leaders described privacy concerns and resource challenges. Participants called for improved infrastructure, communication, and more mental health and exposure data. Firefighters were resistant to using biometric data from wearable devices on calls, citing autonomy and privacy concerns, whereas leadership supported this use

case. Participants described barriers to implementation and conditions for acceptable wearable use, including limiting use cases and data access, sharing individual data with firefighters, and communicating the purpose and benefits to firefighters.

Conclusions: Data and wearable technology have the potential to contribute to firefighter health and safety but must be utilized in a way that protects firefighter autonomy and privacy. Unions could play a key role in negotiating for data privacy protections. Government officials and fire departments can help ensure ethical use of firefighter data by integrating privacy protections into data infrastructure and wearable interventions. Future research should fill data gaps and foster trust in data by communicating research results back to firefighters.

Advisor: Cassandra K. Crifasi, PhD, MPH

Readers: Joseph Ali, JD
Shannon Frattaroli, PhD, MPH
Paul Locke, DrPH, MPH, JD

Alternates: Alexander D. McCourt, JD, PhD, MPH
Danielle German, PhD, MPH

Acknowledgements

I owe sincere thanks to the firefighters who lent their time and ideas to this work. Firefighters are busy providing their communities with essential—and often life saving—services. I am indebted to the firefighters who took time from their days to speak with me and let me tag along on ridealongs. Thanks to the leaders in each department who facilitated this work, and particular thanks to my points of contact in each department who advocated for this study and coordinated data collection.

Many people have told me that I have the dream advisor and I couldn't agree more. Thank you to Cass Crifasi for your mentorship, patience, encouragement, and for making the PhD feel fun, exciting, and as close to easy as possible. Thanks to Cass and my committee members, Shannon Frattaroli, Joe Ali, and Paul Locke, for providing me with such kind, encouraging, and insightful feedback along the way. A huge thank you to Jenn Taylor for introducing me to the fire service, to fire departments, and for championing my work. This study would not have been possible without Jenn and her team. Thanks to these faculty and others I have worked with who taught me so much through RA and TA experiences, sat on exam committees, and offered words of wisdom over the last few years, particularly: Beth McGinty, Colleen Barry, Adam Levine, Hahrie Han, Beth Resnick, Shelley Hearne, Kadija Ferryman, Danielle German, Alex McCourt, Jon Vernick, and Alene Kennedy-Hendricks. I am so grateful to Aleks Wec for helping with Aims 2 and 3, which are much stronger thanks to her perceptive ideas and keen eye for detail. Thanks to Christina Bailey, Judy Holzer, and Mary Sewell for helping me sort through data collection and academic logistics.

I am so lucky to have gone through this PhD with a brilliant and kind cohort: Lois Dankwa, Ross Hatton, Andrew Jopson, Angela Liu, Nick Meyerson, Jenni Seale Reiff, Justin Rose, and Rachel Wu. It is hard to believe that we first met masked in parks and got to know each other on Zoom. Thanks to each of you for the thoughtful ideas, encouragement, walks, meals, coffees, and happy hours that have fueled these years. I am grateful to have found enduring (and now face-to-face) friendships in this group. Special thanks to Carla Tilchin for literally sitting by my side in Hampton House as I wrote and for the words of wisdom, laughs, and commiseration. Huge thanks to Elizabeth Stone for passing along all the essential advice and novel recs that I needed along the way. Thanks to the pickleball crew—Alexa Bellows, Audrey Buckland, Greg Rosen, and Bettina Wunderlich—for the venting, gossiping at the net, and toasting to large and small milestones. Thank you to many other friends near and far for making me laugh and for giving me joy and encouragement the last few years: Elizabeth Graham, Gabby Headrick, Lais Miachon, Cedric Al Kazzi, Jenny Markell, Rebekah Wold, and Camille Morgan. Thank you for making this PhD so much more fun than I ever expected it could be.

Thanks to my family for their encouragement and support, through phone calls across time zones, cooking (the ultimate love language), and visits to Baltimore from across the globe. Thank you to my parents for modeling what it looks like to do meaningful work while finding meaning in other important areas of life. Thank you to my sisters for talking through challenges large and small and for cheerleading when I needed it. And finally, thank you to Simon for your love and support. I can’t wait for our next chapter together.

Funding

This dissertation was supported by the National Institute for Occupational Safety and Health and the Johns Hopkins Education and Research Center for Occupational Safety and Health (T42 OH0008428), the Center for Qualitative Studies in Health and Medicine, and the Susan P. Baker Scholarship in Injury Prevention and Control.

Table of Contents

List of Tables

List of Figures

Chapter One: Introduction

Firefighters operate in hazardous environments and experience high rates of occupational injury, yet remain an understudied worker population[1,2] While new data surveillance systems and technologies present opportunities to protect firefighter health and safety, their success will hinge on firefighter acceptance and implementation that honors firefighters' preferences.[3,4] No studies to date have explicitly examined firefighter perspectives on data privacy or determined where their preferences align with their employers or public policies. These information gaps will only grow as new technologies are deployed. This dissertation examines the policy environment governing firefighter health and safety data and fire service stakeholder perspectives to establish a baseline understanding of their preferences, determine if policy reforms are needed, and inform the ethical collection, use, and sharing of firefighter data.

Literature review

Occupational health and safety data

Protecting worker health and safety remains an ongoing challenge in the United States. In 2022, the Bureau of Labor Statistics (BLS) reported 2.8 million nonfatal workplace injuries and illnesses, and an additional 5,486 fatal work injuries.[5,6] While injury rates have fallen over time,[7] workers in high-risk fields continue to face occupational hazards that threaten their wellbeing and impose cost burdens estimated at over $170 billion annually.[8]

As injury rates have fallen, employers and occupational safety professionals have begun to explore new injury prevention strategies.[9–11] These proposals often involve the collection of large amounts of data or rely on new technologies. Many existing technologies focus on worker monitoring, such as devices tracking truck driver fatigue, or belt monitors for warehouse workers that send alerts based on lifting technique and posture.[12,13] Other advancements remain in development stages and depict futuristic visions of exoskeletons and implantable sensors that could collect extraordinary amounts of personal data.[14,15] The advancement of these technologies signals a new era of worker surveillance that has sparked data privacy concerns.

Regulation of occupational health and safety data

The advances in occupational data surveillance and associated technologies are occurring within a complex but loose regulatory space. Workplace safety initiatives, the data they generate, and any technology involved may be subject to regulations. From a federal standpoint, the Occupational Safety and Health Administration (OSHA) issues guidance on designing and implementing effective safety programs, but has no formal requirements for such programs.[16,17] Programs are presumably designed in accordance with OSHA's General Duty Clause, which requires employers to operate workplaces free from recognized hazards,[18] and must comply with policies related to employment and health.[19–21]

Data collected in a workplace safety program is covered by a patchwork regulatory system governing employers, technology used to collect the data, or the data itself. Employers are

subject to federal regulations governing employee monitoring such as the Electronic Communications Privacy Act of 1986, and are required to keep medical information confidential under the Americans with Disabilities Act.[19,21] Employers may also be required to obtain consent to collect or use data, or to offer deletion rights, under international regulation such as the General Data Privacy Regulation or state-specific laws.[22,23] Technology used in workplace safety programs and the subsequent data collected are often exempt from federal regulation of health information, as most employers are not HIPAA-covered entities and many wearables are not considered devices so long as they are low risk and intended for general wellness.[24,25]

Collectively, these policies, a worker's terms of employment, and the architecture of private sector privacy policies default to a "notice and choice" data privacy framework. Under notice and choice, individuals are provided notice of data collection and asked to consent to the terms provided.[26,27] Privacy experts are critical of this framework, in which users face inherently constrained choices, and there are growing calls to implement employer- or sector-specific reforms.[26–28] Research on consumer behavior suggests that users often do not understand the terms they agree to or may accept terms counter to their stated preferences.[29–34] This phenomenon may be exacerbated in occupational settings, in which workers seeking employment or participating in a safety initiative face limited choices. Understanding how workers and leadership view the notice and choice framework and other relevant policies will help inform the development of future privacy reforms.

Employer and employee perspectives

The literature on general attitudes towards data and technology in occupational settings reveals well-documented and long running concern about employee data privacy, driven by the advent of technologies and policies that allow for substantial monitoring of workplace activities.[26,35–37] Studies have discovered employee privacy concerns related to a range of technologies, including video monitoring, electronic communication tools, and location tracking.[35,38–40] Evidence suggests that workplace surveillance is most threatening for vulnerable worker populations such as contract workers, lower earners, and racial minorities.[26,35] These subpopulations may be more likely to be monitored, pressured into accepting surveillance, or be failed by the technology itself (e.g. facial recognition programs that operate poorly for racial minorities). There is also a growing body of work highlighting privacy concerns specific to data collected for the purpose of improving safety outcomes, often examined through the lens of new technologies. While much of the literature consists of normative work outlining ethical frameworks, there are increasing calls for empirical investigations, and several studies offer initial insights on worker and employer views.[9,41–44]

Emerging scholarship on employee perspectives suggests that workers are broadly concerned about privacy issues in safety contexts.[35] A 2019 survey examining employee willingness to use wearables across sectors and use cases found generally favorable views that vary based on factors such as application, organizational characteristics, and individual demographic characteristics.[45] Participants were more likely to express willingness to use a wearable for safety-oriented purposes if the wearable would only be used during, and not outside of work. Individual characteristics such as positive safety climate perceptions, past wearable use, union

membership, younger age, self-reported Black race, and being male were positively associated with wearable use. Several characteristics were associated with lower likelihood of wearable use, including having a lower income, being a frontline worker (compared to supervisor), self-reported Asian race, and having prior privacy or data security concerns.

Research on employer views across sectors indicates that they are optimistic about deploying new monitoring or surveillance technologies to improve safety outcomes, but that they share employees' data privacy hesitations.[10] Employers also express concerns about adoption related to adherence and cost-benefit considerations, illustrating the range of implementation challenges these technologies pose.

Firefighter health and safety data

Firefighters experience high rates of injury: the National Fire Protection Association (NFPA) reported over 65,000 on-duty firefighter injuries and 96 on-duty fatalities in 2022.[1,2] While firefighters face inherently dangerous conditions when actively managing fires, a majority of injuries (65%) occur outside of firegrounds, including at non-fire incidents, while training, or while traveling to or from an incident.[2] Strain, sprain, or muscle pain injuries were a leading cause of injury both on and outside of firegrounds.[2] Fatalities were primarily linked to overexertion and stress, with sudden cardiac events accounting for nearly 40% of fatalities in 2022.[1] Beyond on-duty injuries and fatalities, firefighters routinely encounter occupational hazards that are associated with increased risks of adverse health outcomes. Firefighting as an occupation has been labeled a carcinogen, and there is rising concern about occupational

cancers among firefighters.[46–48] Occupational illnesses, injuries, and fatalities place enormous personal burdens on firefighters and their communities, and impose significant financial burdens on individuals, fire departments, and their jurisdictions. Researchers estimate that nonfatal injuries alone result in annual economic costs ranging from $1.9 billion to $5.9 billion, with an estimated average cost per injury of $95,000.[49]

There is growing interest in harnessing data and technology to reduce firefighter injuries and fatalities.[3] Proposals call for strengthening existing data collection systems to enhance our understanding of firefighters' occupational safety and design interventions accordingly. Current surveillance efforts are hindered by incomplete reporting and data management challenges. Researchers highlight gaps in data reporting to existing burn and cancer registries, hindering efforts to estimate injury rates, provide effective care, and devise new prevention strategies.[50,51] There are growing calls to strengthen data surveillance systems and leverage data linkages to better understand firefighter injury rates and inform injury prevention efforts.[52] These efforts are already well underway: NIOSH plans to launch the National Firefighter Registry (NFR) in 2022 to monitor and analyze occupational risk factors for cancer.[53] And in 2023, the U.S. Fire Administration announced that it would develop a new incident reporting system, the National Emergency Response Information System (NERIS), that could include injury reporting capabilities.[54]

Beyond national-level data systems, there is growing interest among researchers and government entities in firefighter monitoring and surveillance conducted via emerging

technologies such as mobile apps, sensors, or wearables.[3,55,56] A systematic review of novel firefighter technologies describes a wide array of tools including data systems, communication tools, unmanned vehicles and individual firefighter augmentation.[55] These technologies have the potential to collect enormous amounts of data. Sensors embedded in clothing or wearable devices can collect biometric data tracking a firefighter's heart rate, blood pressure, temperature, respiratory rate, ergonomics, and hazard exposure.[3,56] Mobile apps can track geographic location in real time for incident commanders and integrate information from multiple data sources such as a sensor network.[55,57] Data could be collected and analyzed later or communicated in real time during an incident to forecast injury risk.[3] In addition to generating large swaths of data, these tools may facilitate broader data sharing, both between an individual firefighter and his/her employer, as well as government entities, researchers, and technology companies.

Firefighter perspectives on data privacy and technology

Despite the potential for new technological tools to improve worker health and safety, their success will depend in part on firefighter acceptance. Fire service researchers acknowledge that new data systems and monitoring technologies raise privacy concerns.[3,58,59] A 2015 NIST research roadmap on the use of technology in firefighting called for additional research into the privacy concerns these advances raise, including research on how concerns will manifest and how to design programs and policies accordingly.[3] However, few studies directly examine firefighter perspectives on data and technology or how their perspectives align with management views or the current public policy landscape.

Several studies have assessed data privacy perspectives in the fire service through the lens of new technologies. A 2008 study surveyed firefighters in the southwestern United States to develop and validate a construct to predict how privacy concerns and self-construal affect views towards biometric data collection.[58] The authors found that distrust in biometric data storage, use, and sharing were negatively associated with trust in biometrics; this implies that firefighters' have concerns about biometric data collection, which may extend to data collection of personal information more broadly. A qualitative study examining firefighter perspectives on a pilot of a new wearable biometric device found that firefighters were skeptical of the technology as it would limit their autonomy at incident sites, reinforce a hierarchical culture, and threaten their sense of identity and commitment.[59] However, leadership was more supportive and noted the potential for real time tracking to identify firefighters who were reaching their limits. Another study conducting case studies on personal protective equipment (PPE) highlighted theoretical privacy concerns, but did not solicit perspectives from firefighters or leadership.[4]

While these studies offer insights into firefighters' data privacy concerns surrounding specific devices, no studies to date have comprehensively evaluated individual firefighter or leadership's data privacy preferences, or the motivations underlying these perspectives. The results from other workplace settings suggest that while firefighters might generally support data collection and technology aimed at improving safety, their work environment and individual sociodemographic characteristics may influence their privacy preferences. Trends from other

occupational settings may differ in the fire service or be exacerbated. For instance, the privacy threats that minority populations face may be particularly pernicious in the fire service, which is predominantly white and male: according to the Bureau of Labor Statistics, 88% of employed firefighters identify as White race/ethnicity, and only 4% of employed firefighters identify as female.[60] Overall, existing research suggests that firefighters and their employers may have data privacy concerns related to the reporting of personal health information or injury data, and may hesitate to fully endorse initiatives that increase data collection without appropriate privacy protections.

Specific aims

This study examines the public policy environment and firefighter and leadership perspectives on data privacy in the fire service. This dissertation is composed of three specific aims:

1. Characterize the public policies regulating firefighter data collection, use, and sharing in the context of workplace health and safety.
2. Determine firefighter and fire service leadership perceptions of current occupational health and safety data collection, use, and sharing practices.
3. Understand firefighter and fire service leadership attitudes towards future health and safety data collection using wearable technologies.

Conceptual framework

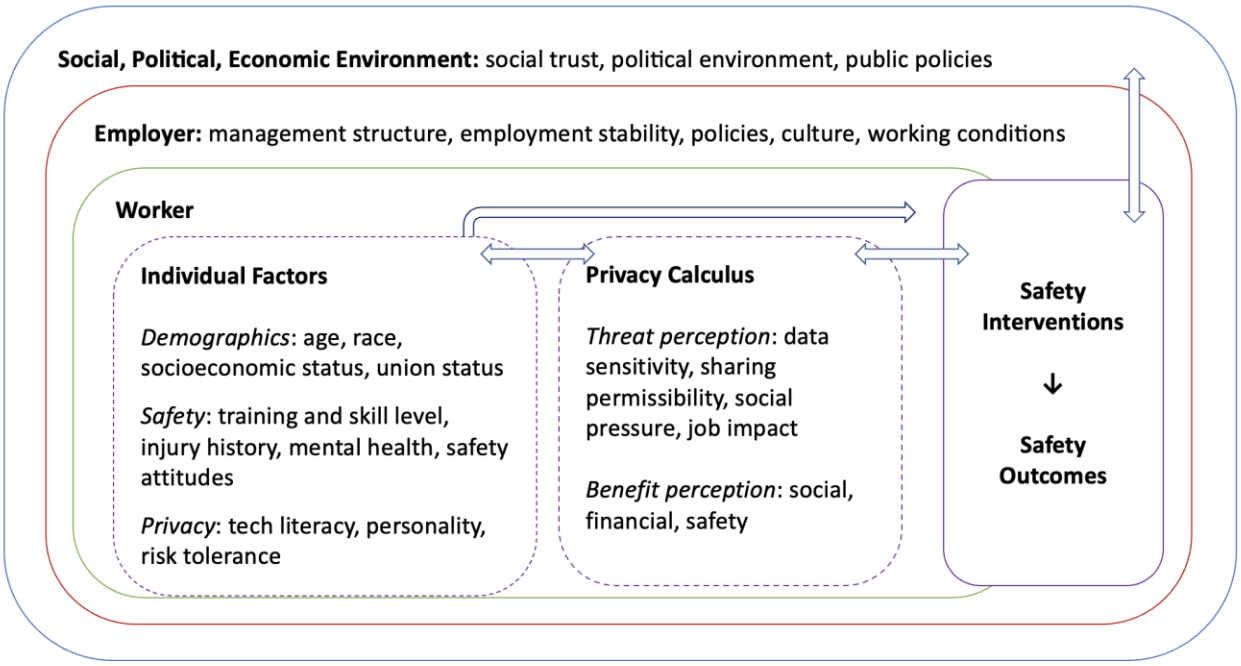
This study integrates research and theories from several fields, most notably occupational safety and data privacy. Occupational health and safety frameworks examine the factors shaping worker outcomes. Models such the Sorensen et al framework for work, safety, health and wellbeing, include individual worker characteristics, employer characteristics, and the broader sociopolitical environment in which workers and their employers operate.[61] The Sorensen framework consists of four concentric circles that reflect distinct levels of influence on worker outcomes: social, political and economic environment; employment and labor patterns; enterprise factors, and worker characteristics. The enterprise and worker domains are subdivided into additional categories. The enterprise level includes workplace policies, programs, and practices that affect the conditions of work, which in turn affect enterprise outcomes. The worker level includes individual characteristics influencing safety, health, and wellbeing characteristics, activities, and outcomes; these in turn shape enterprise outcomes.

This model presents a holistic view of worker safety and captures important workplace and worker characteristics that influence safety outcomes, such as the physical and psychosocial work environment and individual demographics, training and skills, and union status. It places particular emphasis on enterprise factors like the physical work environment and outcomes such as turnover, productivity, and costs. While these are important components contributing to workplace safety and health, the worker lens is deprioritized relative to employer-level factors.

Data privacy frameworks are typically designed to reflect online information disclosure or decisions to adopt new technologies requiring data sharing, and capture the factors informing data sharing preferences. These models, such as those proposed by Li,[62] describe a range of factors that inform an individual's privacy calculus, which ultimately determines intention to disclose information and actual disclosure. The Li framework presents an integrated framework for online information privacy research. It depicts several stages through which an individual makes a decision to disclose information: threat appraisal, a risk calculus, a privacy calculus, an intention to disclose, and ultimately disclosure behavior. Threat appraisal is determined by myriad social and individual factors such as social trust and individual personalities. This baseline threat perception in turn shapes the risk calculus, in which a person weighs the costs of disclosing information. An individual weighs these risks and benefits by making a privacy calculus, which determines their attitudes and intentions towards disclosure. This is eventually manifested in an actual disclosure (or not), which is also shaped by perceived control and self-efficacy. This framework, which was designed to examine online consumer information disclosure, includes additional elements related to behavioral theory that are less relevant for this study, but it offers a helpful model for understanding the factors that determine privacy attitudes.

The model for this study (Figure 1.1) merges these frameworks to emphasize the worker perspective and show the relationships between worker characteristics and data privacy preferences, employer considerations, the sociopolitical environment, and safety outcomes.

Figure 1.1. Adapted conceptual framework for data privacy in occupational safety settings



This adapted model retains the concentric circles from the Sorensen et al model but collapses the employment and labor patterns category into the two categories surrounding it: the social, political, and economic environment and the employer level. The outermost circle, which focuses on the social, political, and economic environment, incorporates public policies and the political environment, which determine an employer's safety obligations and shape workforce trends. This circle also includes social trust, reflecting the Li framework's emphasis on the social environment that informs privacy and disclosure preferences. The employer circle reflects workplace features that impact both safety and workplace trust, such as management structure, culture, and working conditions.

This model devotes the most attention to the worker level to center the worker in safety and privacy discussions. Individual factors include demographic characteristics, safety characteristics such as training, injury history, and safety attitudes, and privacy elements such as tech literacy, personality, and risk tolerance. These both directly shape safety interventions and outcomes, and inform a worker's privacy calculus. The privacy calculus focuses on threat and benefit perceptions. Threat perceptions are informed by the nature of the data collected, sharing, social pressures, and perceived influence on day-to-day work. Perceived benefits can be social, financial, or safety-related. This privacy calculus, which can also affect individual characteristics such as an individual's risk tolerance or safety attitudes, affects safety interventions and outcomes. An individual's willingness to share personal information, participate in a research study, or pilot new safety initiatives, all impact the success of a safety intervention and its eventual effect on outcomes.

Aim 1 unpacks the policy environment governing firefighter occupational health and safety data. This Aim addresses the outer circle in the model that shapes each other element including employer- and worker-level factors. Aims 2 and 3 examine the worker and employer levels by interrogating firefighter and leadership perspectives on data privacy. These aims assess preferences related to information sharing with employers, researchers, and government entities, reflecting the links between the employee, employer, and broader social and policy domains.

Dissertation organization

This dissertation contains three manuscripts and a concluding chapter. Chapters 2-4 consist of one manuscript for each study aim. Chapter 5 summarizes the findings and implications for practice, policy, and research. Tables are included within each manuscript, and supplementary materials are included in the overall Appendix that follows the chapters.

Chapter Two (Manuscript One): Firefighter occupational health and safety data privacy: an analysis of statutory, regulatory and contractual governance mechanisms

Abstract

Objective: There is increasing interest in collecting occupational health and safety data to protect workers in high-risk fields such as firefighters. However, there is limited research examining the public policies governing this data. We carried out an initial review of the policies that impact firefighter occupational health and safety data in Maryland and Virginia.

Methods: Given the paucity of studies about the laws, regulations and policies governing firefighter data and privacy, we analyzed a subset of these categories. Our landscape analysis borrowed techniques from traditional legal and policy analyses. We identified a subset of laws, regulations and union contracts at the federal level, and in Maryland and Virginia in three domains: labor, health and safety, and data privacy. Data collection took place using secondary sources and the Westlaw legal database from March 2023-May 2023. We analyzed policies using a data abstraction tool capturing data privacy parameters and developed a framework for analyzing the strength and breadth of these policies.

Results: Our landscape analysis reviewed 20 laws and regulations: nine federal, three in Maryland, and eight in Virginia, and 11 union contracts. We developed a framework identifying factors for organizing or evaluating data privacy policies: permissiveness of data collection, data use or purpose, storage conditions, and sharing or access privileges. Our review revealed few

laws and regulations that directly relate to occupational health and safety data privacy, and only two fire service-specific laws. Federal policies comprehensively address data privacy factors. Both states have data privacy-oriented laws. Union contract data protections vary, with many imposing limits on access to sensitive data, while others authorize electronic surveillance.

Conclusions: Based on this initial review, we conclude that the current legal structure provides some protection against the unauthorized release and use of occupational health and safety data. Additional policymaking would be needed to further safeguard firefighter health and safety data. State and union policies could serve as a model for future policymaking across jurisdictions. Researchers and advocates can contribute to the policymaking process to ensure policies adequately protect worker data while limiting burden.

Introduction

Firefighters provide essential public services. Despite experiencing high rates of injury and their important societal role, they remain an understudied worker population from an occupational safety and health perspective. In 2021, the National Fire Protection Association reported over 60,000 on-duty firefighter injuries and in 2022 there were 96 on-duty firefighter fatalities.[1,63] Fire service researchers consistently highlight the need for more sophisticated data collection and analysis,[3,50–52] and propose using new software platforms or wearable technology to understand and prevent injuries and fatalities.[9,11] Government agencies are leading efforts to strengthen national surveillance: in 2023, the National Institute for Occupational Safety and Health (NIOSH) launched the National Firefighter Registry for Cancer and the U.S. Fire Administration announced that it will create a new data analytics platform.[54,64]

Fire service researchers recognize that while more robust data collection may improve health and safety it also prompts privacy concerns.[3] There is relatively little research on data privacy in the fire service, but one study examining views towards wearable devices documented divergent views between firefighters who feared adverse impacts on their work, and leadership who identified safety benefits.[59] This is consistent with the broader literature on health and safety data in employment settings, which typically examines attitudes towards new technologies. Researchers have identified broad support for technology among employers while employees express privacy concerns.[10,45] In addition to this tension, it is unclear how occupational health and safety data is currently regulated, and whether existing policies adequately protect against disclosure of personal health and safety data. Privacy scholars

express concern over workplace surveillance and criticize the lack of policies protecting workers from monitoring.[26,65] However, there is little to no research that comprehensively examines the policies dictating how occupational health and safety data is collected, used, stored, and shared in this domain.

As discussion about more sophisticated and increased data collection continues, it is essential to understand how this data is currently regulated and examine whether current policies sufficiently protect firefighter data. In this paper, we identify a subset of the current laws and regulations governing firefighter occupational health and safety data privacy at the federal level and in Maryland and Virginia, as well as state and local union contracts in Maryland and Virginia fire departments. We use these findings to develop a framework for understanding the nature of data privacy policies and assess the policies in each jurisdiction. To our knowledge, this is the first study to assess the policy environment for this topic and population. Our findings offer an initial overview of the regulatory landscape for firefighter health and safety data and can be utilized to identify gaps and opportunities for future policymaking.

Methods

Our method of analysis drew upon techniques from traditional legal and policy analyses to identify federal, Maryland, and Virginia laws and regulations related to firefighter occupational health and safety data. We selected these states for two reasons. First, Maryland and Virginia are neighboring jurisdictions and many fire departments have mutual aid agreements facilitating assistance across state lines, but the states have different labor laws environments.

We anticipated differences across these two states that might reveal a wider range of policies. Second, we plan to conduct future empirical work in these states to understand fire service stakeholders' perspectives towards data privacy.

We examined laws and regulations in three domains: labor, health and safety, or data (i.e. laws or regulations addressing the collection, storage, use, or sharing/access of employee or firefighter information). We excluded guidance documents that are not legally enforced. Because of our emphasis on workplace data, we defined firefighters as career (sometimes referred to as paid) firefighters. We conducted a two-stage data collection process using the Westlaw legal database to identify laws and regulations. In the first stage, we queried secondary sources in Westlaw to identify law review articles that discussed relevant laws and regulations, using search terms related to data privacy, health and safety, and labor or employment.[26,66,67] We also relied on the Westlaw Practical Law Employee Privacy Law resources for Maryland and Virginia.[68,69]

In the second stage, we conducted targeted searches of laws and regulations. For each jurisdiction, we used standardized search strings that covered at least two of our three domains: labor, health and safety, or data (see Appendix 2.1 for search terms). We conducted searches specific to firefighters and the fire service, as well as searches using general employment terms to capture other labor policies that would apply to firefighters. As we reviewed each law or regulation, we added policies that were referenced and met inclusion criteria. We excluded proposed legislation and rulemaking, laws or regulations specific to non-fire service sectors,

those related to surveillance of non-health or safety information (e.g. email), laws that did not address data, and narrowly scoped laws (e.g. those applying to voluntary protection programs). Regulations inherently flow from laws, and so in some cases we included both a law and an associated regulation if both addressed our topic of interest. In other cases, if a statute did not specifically address data privacy but authorized a broad scope of rulemaking that ultimately led to regulations addressing data privacy topics, we included the regulation but not the law so that we could focus on policies relevant to occupational health and safety data privacy.

To aggregate union contracts, we first identified state and local fire departments reporting "career" or "mostly career" staffing to the U.S. Fire Administration's National Fire Department Registry.[70] We included unionized departments that negotiate contracts with the state of Maryland or Virginia or counties or cities within each state. We then searched for the most recent publicly available contracts (in some cases, expired contracts which have not been renegotiated). In cases where we could not find the most recent contract online, we contacted union leaders and local officials. For one jurisdiction, Annapolis MD, we were unable to obtain a recent contract and excluded it from our analysis. We will refer to "policies" when describing our collective findings.

After identifying relevant policies, we developed a data abstraction tool to examine features such as jurisdiction, covered entities, covered data, and data privacy factors (data collection, data use or purpose, data storage, and data sharing or access). This tool was created in an iterative fashion based on preliminary review of the documents and existing data privacy

frameworks.[27,71] Within each data privacy factor we generated subcategories capturing additional nuance. We reviewed each policy using the data abstraction tool and aggregated the findings across jurisdictions. Data collection took place between March 2023-May 2023.

Results

Data privacy policy framework

While there were variations in the nature of each policy, they typically related to one of four data-related considerations: collection, use or purpose, storage, and sharing or access. Differences within each of these categories reflect the varied design, strength, and breadth of policies across and within jurisdictions. Data collection provisions fell into four subcategories: restrictive, permissive, mandated, or presumed. Some policies limited collection of medical, disability, or genetic information (restrictive), whereas others required the collection of injury or fatality data (mandated). In other cases, laws allowed for collection of information under specific circumstances (permissive), or inherently presumed data collection occurred (presumed). Data use or purpose provisions described appropriate uses of data and reflected the intent of each policy: anti-discrimination, employment benefits, injury surveillance, or data privacy. Anti-discrimination laws prevented data from being used to distinguish prejudicially in employment. Benefits-related policies allowed data to be used to process benefits such as workers compensation or presumptive firefighter benefits, which are intended to ease access to benefits for work-related diseases such as cancer.[72] Injury surveillance policies were designed to track worker illness, injuries, or fatalities, and data privacy policies were explicitly aimed at privacy considerations.

Data storage considerations addressed the location or retention of data. This might include storing medical, disability, or genetic information separately from personnel records, or mandating that data be kept for a specific number of years. Data sharing and access provisions included those that are limiting, required, or encouraged. Some limited access to or sharing of disability, medical, injury, or fatality information, whereas others required reporting of injuries and fatalities to government agencies and/or required that employees may access their own data. A small number of policies encouraged data sharing in aggregate form for educational or prevention purposes.

We use this framework to analyze the strength and breadth of policies we identified. Some policies addressed all four parent categories whereas others addressed only a few. Subcategories are not mutually exclusive: a law might address both location and duration of data storage, or limit sharing while maintaining individual employees' access to their own data.

Overview across jurisdictions

We identified 20 laws and regulations that impact the occupational health and safety data of career firefighters: nine at the federal level, three in Maryland, and eight in Virginia; we also identified nine union contracts in Maryland and two in Virginia. Across jurisdictions, there were three laws or regulations directly aimed at occupational health and safety data privacy, and only two laws directly related to the fire service. Federal laws and regulations more comprehensively addressed each data privacy factor than Maryland and Virginia laws and regulations (Table 2.1).

All nine of the federal policies addressed data collection, use or purpose, and storage, and eight addressed sharing and access. The two states have enacted policies that are more limited in scope. While all addressed data use or purpose, only one Maryland law highlighted data storage, and we did not identify Virginia laws or regulations within our scope of firefighter occupational health and safety data privacy that explicitly discussed data storage. However, while federal policies addressed a range of privacy factors, we did not identify any federal data privacy legislation, whereas the two states have both passed data privacy laws. We found only one federal regulation directly aimed at data privacy in occupational health and safety contexts, but it narrowly applied to OSHA employee access to medical data.[73] On the state level, Maryland had a law requiring secure storage of information including health and biometric data;[74] in 2023, Virginia passed a law authorizing broad future data privacy rulemaking.[75] Table 2.2 provides an overview of each data privacy policy provision.

At the union level, we identified more collective bargaining agreements in Maryland than Virginia (Table 2.3). Union contracts varied in scope, with most addressing collection of injury, exposure, or sick leave information for injury surveillance or benefits. Three Maryland contracts limited sharing of and access to medical or injury information and two required firefighters have access to their own information.[76–79] In Virginia, Alexandria's contract required that employees report injury information and that the department share personal exposure reports with employees. In Arlington, the contract included a range of provisions limiting access to sick leave, medical, and injury information while requiring that employees have access to their own data. Both Virginia contracts authorized electronic monitoring for health and safety purposes without

imposing storage or sharing limits.[80,81] Table 2.4 details each contract's data privacy provisions. Appendix 2.2 contains detailed summaries of all policies.

Overview by jurisdiction

The bulk of federal laws and regulations we identified either established injury and fatality reporting requirements or prevented sensitive data from being used in discriminatory fashion in employment. Five of the nine federal policies required reporting of injury or fatality data, including the Federal Fire Prevention and Control Act of 1974, which established epidemiological surveillance of firefighter injuries and fatalities.[82–86] This law mandated the creation of the National Fire Data Center to conduct voluntary reporting of firefighter fatality and injury data. The law required that the Data Center collect information on serious fatalities (those requiring medical treatment by a doctor), deaths occurring while preparing for work or a test, and injuries and deaths from motor vehicle and aircraft accidents. A smaller number of federal laws restricted collection of medical, disability, or genetic information to prevent discrimination in employment,[87,88] and one allowed for collection of medical information to process Family and Medical Leave Act (FMLA) benefits.[89] All of the policies addressed the location and retention of data; the Americans with Disabilities Act (ADA) and Genetic Information Nondiscrimination Act (GINA) required that medical and disability information be stored separately from personnel files.[87,88] Four of the policies limited access to and sharing of medical and disability information,[73,87,88,89(p29)] whereas three encouraged or required reporting of injury and fatality information (including individual employees' access to their own data).[83,85,86(p29)] The lone fire service law encouraged sharing of aggregated firefighter injury and

fatality data collected by the National Fire Data Center.[82] These federal laws and regulations also applied at the state level. While federal OSHA does not necessarily cover state and local employees like firefighters, if states voluntarily enact their own OSHA plans as Maryland and Virginia have, then federal standards apply.[90]

Of Maryland's three statewide policies, two were similar to federal laws. One law barred the discriminatory collection of disability information in employment contexts, although unlike the ADA, it did not contain storage, sharing, or access stipulations.[91] A regulation addressing employee injury and illness records required that employers report illnesses, injuries, and fatalities to Maryland's OSHA office (MOSH) but similarly lacked storage requirements. The Personal Information Protection Act, a data privacy law, emphasized data security, requiring secure storage (generally defined) of employee information, including health and biometric information; it also required that employees be notified if their information is breached.[74]

Virginia's eight statewide policies encompassed a range of data provisions, including injury and fatality reporting, benefits, limiting data access, and ensuring employees' data rights. Two statutes required reporting of injury and fatality data to the state Department of Labor and Industry (DOLI) and/or workers compensation commission for injury surveillance or to process benefits.[92,93] A fire-specific bill establishing presumptive benefits for firefighters allowed employers to collect medical information to confirm eligibility.[94] Several other policies addressed access to employee health and injury data, including a regulation that imposed limits on health professionals and the labor commissioner accessing employee records[95] and a law granting employees the right to access their own injury data.[96] These protections are echoed in

a consumer genetic testing law specifying that direct-to-consumer (DTC) companies cannot disclose consumer data to entities making decisions about employment without the consumer's consent.[97] Virginia also laid the groundwork for future data privacy rulemaking: a 2023 law authorized the creation of a state Chief Data Officer and authorized extensive rulemaking, specifically around data collection, use, storage, sharing, and other privacy concerns related to data collected or maintained by state, regional, or local public entities.[75]

Several collective bargaining agreements in Maryland addressed data related to physical exams, medical exams, or injuries, for the purposes of certifying leave or encouraging health and fitness. However, over half did not address storage or access/sharing,[79,98–102] whereas three placed limits on who can access medical information and required that employees be able to access their own data.[76–78] Montgomery County had the most comprehensive contract, which covered sick leave, injury, and medical information, but also specified that the department must collect fitness records. It also included detailed access and sharing provisions, mandating that fitness data must be treated as confidential and not shared outside of the fitness team, and that employee assistance program (EAP) information must not be shared without written consent from an employee.[78]

As in Maryland, Virginia's two union contracts addressed recordkeeping requirements for injury and exposure data, as well as regular physical examinations.[80,81] However, both contracts authorized broad use of electronic monitoring device data, with Arlington specifically allowing such data to be used for health and safety purposes. The Arlington contract authorized

Arlington County use of video, audio, or other electronic monitoring. Employees must be notified of audio and video recording, and the County could not proactively use this data to identify policy violations. However, the contract specifically stated that "The County shall utilize video, audio, and data streams to … improve the health and safety of employees, conduct training and professional development, facilitate promotional examinations, and perform research or investigations."[80] While both Virginia contracts addressed access and sharing more generally, they did not include specific language regarding how this kind of electronic surveillance data might be accessed, shared, or stored within fire departments.

Discussion

Our research identified a range of policies governing occupational health and safety data, highlighting strengths and gaps in the existing regulatory framework protecting firefighters federally and in Maryland and Virginia. We identified only one narrowly scoped federal regulation specifically addressing employee occupational health and safety data privacy: 29 CFR § 1913.10 Rules of Agency Practice and Procedure Concerning OSHA Access to Employee Medical Records.[103] This regulation applied only to OSHA staff, and did not apply to employers, researchers, or commercial entities that frequently obtain employee data. Although we identified several federal-level policies that required the collection of serious injury and fatality data, laws and regulations requiring the reporting of injuries and fatalities failed to address access or sharing concerns, instead encouraging the sharing of aggregated data. While publishing injury and fatality trends is essential for understanding and improving workplace health and safety, public policies should ensure that the reporting of such information does not

threaten worker privacy. These safeguards will become even more essential as technology advances. With the advent of sensors and wearable devices, employers could begin to collect highly sensitive data, including biometric information, in greater quantities than ever before.[3]

On the federal level, our review included GINA but excluded the Health Insurance Portability and Accountability Act (HIPAA). These two laws are commonly cited in data privacy discussions[27,71] but we found that they have limited applicability to our topic of interest. HIPAA only applied to covered entities and their associates; employers and employee data collected in an occupational context are not covered by HIPAA.[71,104] GINA has implications for employee health and safety data, as its provisions addressed genetic information broadly defined (e.g. information from genetic tests of the employee or family member; family medical history). This offers some protections for employee health and safety data, such as firefighters' personal or family medical histories, which might arise during annual physicals or fitness for duty assessments. However, GINA included several exceptions through which employers may collect genetic information, including through voluntary workplace wellness programs and when monitoring toxic substances.[71,87] Employers might gain access to sensitive information depending on the circumstances under which they obtain genetic information, although in these cases employers would still be prohibited from using such information in discriminatory fashion. This emphasis on preventing discriminatory use of genetic information might be sufficient for ensuring such data is not used inappropriately, but employees might prefer stronger prohibitions on the collection of such data in the first place. And while GINA protected a broad array of genetic information, it may not address the full range of health information

covered in other contexts (e.g. HIPAA in health care settings), reflecting gaps in federal data privacy policies in occupational settings.

There are ongoing opportunities to shape federal policy through rulemaking. For example, in spring 2022, OSHA issued a proposed rule, "Improve Tracking of Workplace Injuries and Illnesses" that proposes electronic submission of injury data, and public posting of de-identified injury data.[105] The agency specifically requested comments about how to prioritize transparency while managing employee privacy concerns, suggesting that future rulemaking might attempt to address privacy issues. State policies such as those we identified in Maryland and Virginia could serve as models to inform future federal policymaking. From a fire service standpoint, in May 2023, the U.S. Fire Administration announced that it will transition from its legacy injury surveillance system, the National Fire Incident Reporting System (NFIRS), to a modernized platform, the National Emergency Response Information System (NERIS).[54] NERIS, which fulfills statutory requirements of the Federal Firefighting Control Act, will modernize and streamline the fire service's data procedures. Policymakers should consider how to design this platform in ways that respect firefighter data privacy and incorporate input from a diverse array of fire service stakeholders on appropriate data protections.

On the state level, Maryland and Virginia serve as two distinct examples. Virginia's occupational data privacy laws and regulations appeared to be stronger in quantity and quality, but it had fewer collective bargaining agreements, and they authorized broad electronic monitoring of firefighters. Despite the breadth of Virginia's existing policies, we did not identify laws or

regulations addressing the storage of occupational health and safety data, and only Arlington's contract addressed storage. Virginia may want to consider enacting uniform policies for where and how employee occupational health and safety information is stored. The small number of union contracts is likely due to historic labor laws in the state. Virginia is a right to work state, and until 2021, public employees were banned from engaging in collective bargaining.[106,107] In 2023, Alexandria ratified the first firefighter contract in the state in over 40 years, quickly followed by Arlington.[107–109] While Arlington's contract prohibited the department from conducting proactive searches of electronic monitoring data for discipline or retaliation, both contracts allowed for review of such data as part of an investigation. Neither contained specifications for how such data should be stored or who may access or share the data. These unions, and unions attempting to negotiate for the first time in Virginia, could advocate for stronger data protections in future contracts.

Maryland's firefighter data privacy protections are primarily found in union contracts. Maryland's data privacy law included general requirements that data be stored securely, and was amended to specifically cover health and biometric information, which could serve as a model for sophisticated biometric data storage policies.[74] However, this legislation did not address other key data considerations such as data collection or sharing. The state should consider adopting public policies that address these factors or, like Virginia, emphasize employees' rights to access and/or disclose their data. Several of Maryland's collective bargaining agreements build on state and federal policies by limiting fire department personnel access to sensitive information such as medical, injury, or fitness data; jurisdictions without

these protections may wish to incorporate them in future negotiations. While none of Maryland's contracts explicitly authorized the kinds of electronic surveillance included in Virginia's contracts, Maryland union leaders may wish to consider how to protect firefighters' privacy if surveillance arises in future negotiations.

Our findings are consistent with the conclusions of data privacy law experts who criticize the lack of federal data privacy legislation and call for the development of privacy-oriented labor laws .[26,27,71] There is robust debate about the best regulatory approach towards data privacy, as future laws and regulations should protect privacy across multiple populations while not imposing unreasonable administrative burdens. Scholars have also argued that privacy should be viewed an instrumental good—something valuable as a means to other non-privacy goals—meaning that future legislation or rulemaking should also account for non-privacy objectives, such as enhanced worker safety.[27] The path towards comprehensive privacy legislation is complex, as lawmakers could opt for laws applying across worker populations, in the consumer space, or based around kinds of data or technologies. Alternatively, regulators might promulgate new privacy-oriented rulemaking within the bounds of existing legislative mandates, strengthening OSHA's injury surveillance data protections or incorporating privacy safeguards into the Fire Administration's NERIS system. National-level reforms could secure data for large swaths of workers and minimize patchwork protections across states and localities. But national-level policymaking, particularly if aimed at large and diverse populations, faces a host of challenges both conceptual and practical, which might delay advances.

In highly unionized workforces like the fire service,[110] unions may be the most effective advocates for enacting occupational health and safety policies in individual workplaces. Legal scholars have begun to debate the merits of collective bargaining as a pathway for securing privacy protections for the use of wearable technology.[71] Some believe unions are best positioned to negotiate for these reforms, while others point out that this route excludes non-unionized employees or industries. There are few examples of unions addressing wearable technology. Unions representing professional athletes have begun to consider wearable data privacy although experts suggest that most contracts fail to address core privacy issues.[71,111]

In both states we examined, union contracts contained the most granular protections for firefighter data and reflected unique department characteristics and cultures. Union-led privacy reforms are not without challenges; not all departments are unionized, contracts are renegotiated frequently, and contracts can vary significantly, as we observed in our sample in two neighboring states. The collective bargaining process is also unique in that unions negotiating a contract face different pressures and priorities compared to the public policymaking process. While unions might be best equipped to negotiate on behalf of their members, they bear responsibility for other priorities such as obtaining pay raises, insurance benefits, and leave allowances. Public policymaking, which could cover a broader range of employees, offers a more comprehensive pathway towards securing data privacy protections, and might result in stronger and more equitable protections across worker populations and employers. However, policymaking is often a slow process, and there may be tradeoffs between covering a larger array of employees and addressing concerns specific to individual sectors such

as the fire service. In the absence of federal or state legislation or rulemaking, unions can serve as firefighters' best advocates for appropriate data privacy protections. Collective bargaining agreements can also serve as examples of what occupational health and safety data protections should look like in the fire service, and as test cases for ensuring such policies are not overly burdensome. Union leaders preparing for future collective bargaining negotiations should anticipate increased monitoring or surveillance and be prepared to negotiate provisions that protect their members' data privacy and prevent discriminatory use of such data.

Beyond unions, our findings have implications for other stakeholders with an interest in firefighter occupational health and safety data. Researchers, who may not actively engage in bargaining, can help establish an evidence base on firefighters' data privacy preferences. And as OSHA and the U.S. Fire Administration attempt to modernize injury surveillance systems, researchers whose work relies on such data can serve as advocates for expanding access to important data while maintaining the privacy of workers. More generally, our study highlights the need for greater consideration of occupational health and safety data in data privacy discussions. Our findings contribute an exploratory analysis of this topic to the growing literature on worker data and can serve as a starting point for legal experts and privacy advocates to consider as they seek policy reforms.

Our study has several limitations. We did not conduct a comprehensive review of federal, Maryland, or Virginia guidance documents, nor did we include review of federal, Maryland, or Virginia case law. Our scope was narrowly defined to identify the laws, regulations, and union

contract provisions oriented around firefighter health and safety data but did not necessarily capture all of the policies that might govern this data (e.g. state laws dictating how personnel data should be handled more generally). While we examined union contracts, we did not include municipal, county, or fire department policies or procedures that might cover firefighter data. Put simply, our findings are not an exhaustive legal analysis of all the potential policies that could govern firefighter health and safety data. However, to our knowledge, this is the first study to examine this topic and establish an overview of the policy environment surrounding firefighter health and safety data. This exploratory analysis sheds light on existing occupational health and safety data policy protections and highlights opportunities for future research, advocacy, and policymaking. Policy researchers and legal scholars should examine this topic in other states and localities and for additional worker populations. Researchers can also build upon this work by exploring the impact and enforcement of these policies in practice settings.

Conclusion

Career firefighter health and safety data is governed by a patchwork of laws, regulations, and local policies at the federal level and in Maryland and Virginia. While our analysis is preliminary, it demonstrates that these policies address a range of data privacy considerations including data collection, use, storage, and sharing or access, few are oriented around data privacy. This research lends support to calls for additional policymaking to ensure that worker data is adequately protected, and highlights opportunities for advocates and researchers to more effectively engage with the policymaking process. Policies that appropriately safeguard health

and safety data may bolster employees' confidence in injury prevention efforts and ensure that they work in inclusive, healthy, and safe environments.

Table 2.1 Nature of data privacy laws and regulations by jurisdiction

		Federal	Maryland	Virginia
Overall		9	3	8
Collection		8	2	6
	Restrictive	2	1	1
	Permissive	1	0	1
	Presumed	0	1	3
	Mandated	5	0	1
Use/Purpose		9	3	8
	Anti-discrimination	2	1	2
	Injury surveillance	4	1	3
	Benefits	3	0	4
	Data privacy	1	1	1
Storage		9	1	0
	Location	5	1	0
	Duration	6	0	0
Access		8	1	5
	Limited access, sharing	4	1	2
	Required reporting, access	3	1	3
	Encouraged sharing	1	0	0

Notes: some policies address more than one subcategory. “Restrictive” policies limit collection of data. “Permissive” policies allow data collection. “Presumed” indicates that the policies do not explicitly address data collection, but presume it has or will take place. “Mandated” requires data collection.

Table 2.2 Overview of data privacy laws and regulations

	Data Collection Permissions	Data Use and Purpose	Data Storage Parameters	Data Access Provisions	Notes
Federal					
Americans with Disabilities Act, 42 U.S.C. § 12101 et seq.	Restrictive	Anti-discrimination	Location	Limited access, limited sharing	Bars discriminatory collection, use of disability information; storage location; limits sharing to key people
Genetic Information Nondiscrimination Act, 42 U.S.C. § 2000ff et seq.	Restrictive	Anti-discrimination	Location	Limited access, limited sharing	Bars discriminatory collection, use of genetic information; storage location; limits sharing to key people
Family and Medical Leave Act, 42 U.S.C. § 2601	Permissive	Benefits	Location, duration	Limited access, limited sharing	Allows employers to collect medical information for FMLA; storage length and location; limits sharing to key people
Federal Fire Prevention and Control Act of 1974, 15 U.S.C. § 2201 et seq.	Mandated	Injury surveillance	Location	Encouraged aggregate sharing	Requires creation of National Fire Data Center to collect fatality, injury data; encourages sharing in aggregate
Occupational Safety and Health Act of 1970, 29 U.S.C. § 651 et seq.	Mandated	Injury surveillance, benefits	Duration	Required reporting, required employee access	Authorizes DOL to collect fatality, injury, illness, exposure data; requires individual sharing with DOL, employees. Applies to MD, VA firefighters due to state OSHA plans

29 CFR § 1602 Recordkeeping regulation	Mandated	Benefits	Duration	N/A	Requires state, local employers to retain all personnel, employment records for at least two years; one year for unions
29 CFR § 1910.1020 Access to employee exposure and medical records	Mandated	Injury surveillance	Duration	Required reporting, employee access	Requires employers to maintain exposure, medical records; storage length; requires individual sharing with employee, OSHA. Applies to MD, VA firefighters due to state OSHA plans
29 CFR § 1904 OSHA Recordkeeping Rules	Mandated	Injury surveillance	Duration	Required reporting, aggregated sharing, employee access	Requires employers to maintain fatality, injury, illness records; storage length; requires aggregate sharing. Applies to MD, VA firefighters due to state OSHA plans
29 CFR § 1913.10 Rules of Agency Practice and Procedure Concerning OSHA Access to Employee Medical Records	N/A	Injury surveillance, data privacy	Location, duration	Limited access, sharing	Limits circumstances in which OSHA may access employee medical records, imposes privacy-oriented requirements
Maryland					

Personal Information Protection Act, Md. Code Ann. Comm. Law § 14-3504	N/A	Data privacy	Location (security)	Limited access	Requires secure destruction; treatment of data as confidential; requires individual notification in case of data breach
Inquiries Regarding Medical History, Md. Code Ann. Lab. & Empl. 3-701	Restrictive	Anti-discrimination	N/A	N/A	Bars discriminatory collection of disability information
COMAR 09.12.21 Employee Injury and Illness Records and Reports	Presumed	Injury surveillance	N/A	Required reporting	Requires employers to report fatalities, injuries, illnesses; requires MOSH reporting
Virginia					
Va. Code Ann. § 8.01-413.1 Labor and Employment—Records and Recordation—Disclosure	Presumed	Injury surveillance, benefits	N/A	Required employee access	Requires employers to share individual injury data with employee if requested

Va. Code Ann. § 40.1-28.7:1 Genetic Testing or Genetic Characteristics as a Condition of Employment	Restrictive	Anti-discrimination	N/A	N/A	Bars collection of genetic information in employment
Genetic Data Privacy, VA ST § 59.1–593 through 59.1-602	N/A	Anti-discrimination	N/A	Limited sharing	Bars DTC companies from sharing genetic information without consent
Va. Code Ann. § 65.2-900(A) Records and reports of accidents	Mandated	Benefits	N/A	Required reporting	Requires employers to maintain injury, fatality records; required to report to workers comp, insurers, DLOI
Va. Code Ann. § 40.1-51.1(D) Duties of employers	Presumed	Injury surveillance	N/A	Required reporting	Requires employers to report injuries, fatalities to DLOI
Va. Code Ann. § 2.2-203.2:4 Office of Data Governance and Analytics; Chief Data Officer; creation; report.	TBD	Data privacy	TBD	TBD	2023 law authorizes creation of chief data officer. May develop data storage, sharing policies

Presumption as to death or disability from respiratory disease, hypertension or heart disease, cancer, VA ST § 65.2–402	Permissive	Benefits	N/A	N/A	Allows employers to collect firefighter medical information for presumptive benefits
16VAC25-60-80 Access to employee medical and exposure records	Presumed	Benefits, injury surveillance	N/A	Limited access	Imposes privacy safeguards on health professional, labor commissioner access to records

Notes: “Restrictive” policies limit collection of data. “Permissive” policies allow data collection. “Presumed” indicates that the policies do not explicitly address data collection, but presume it has or will take place. “Mandated” requires data collection.

Table 2.3 Nature of union data privacy policies by jurisdiction

		Maryland	Virginia
Overall		9	2
Collection		9	2
	Restrictive	0	1
	Permissive	4	1
	Presumed	4	2
	Mandated	4	2
Use/Purpose		8	2
	Anti-discrimination	1	1
	Injury surveillance	6	2
	Benefits	5	1
	Data privacy	0	0
Storage		2	1
	Location	2	1
	Duration	0	1
Access		5	2
	Limited access, sharing	3	2
	Required reporting, access	4	2
	Encouraged sharing	0	0

Notes: some policies address more than one subcategory. “Restrictive” policies limit collection of data. “Permissive” policies allow data collection. “Presumed” indicates that the policies do not explicitly address data collection, but presume it has or will take place. “Mandated” requires data collection.

Table 2.4 Overview of union data privacy policies

	Data Collection Permissions	Data Use and Purpose	Data Storage Parameters	Data Access Provisions	Notes
Maryland					
Anne Arundel County and IAFF 1563 (2022-2023)	Presumed	N/A	N/A	N/A	Requires the Safety Committee to make recommendations regarding a Personal Exposure Recording Program to document exposures
City of Baltimore and IAFF 734 (2022-2024)	Mandated, permissive, presumed	Injury surveillance	Location	Limited access (employer); required employee access	The department must include exposure reporting to injury reports and share injury reports with the union. Medical file access is limited to select department employees and individual employee access
Baltimore County and IAFF 1311 (2021-2023)	Permissive	Injury surveillance	N/A	Limited access	The department will offer hearing tests, medical exams and physicals, and explore medical screening. Medical exam and physical data will be kept confidential
State of Maryland and IAFF 1742 (2022-2024)	Presumed	Benefits	N/A	N/A	Employees may take temporary unpaid medical leave if it is medically documented; return to work based on State Medical Director declaration

Cumberland and IAFF 1715 (2017-2020)	Permissive	Benefits	N/A	N/A	Requires medical certification from a treating physician or other health care provider to obtain sick leave benefits beyond one shift in length
Hagerstown and IAFF 1605 (2018-2022)	Mandated	Injury surveillance	N/A	Required reporting	Requires fitness for duty physical but does not address storage or access, aside from reporting lack of fitness for duty to HR
Montgomery County and IAFF 1664 (2022-2024)	Mandated	Anti-discrimination, benefits, injury surveillance	Location	Limited access, required employee access	Comprehensive guidance requiring documentation of medical or fitness information to provide benefits, promote health and safety, and prevent injury. Limits access to medical and fitness information and requires employee access to certain records
Ocean City and IAFF 4269 (2019-2024)	Permissive	Benefits, injury surveillance	N/A	N/A	The department may require a physical fitness assessment and medical exam annually. May also require a medical exam to facilitate return to duty following injury or illness

Prince George's County and IAFF 1619 (2022-2024)	Presumed, mandated	Benefits, injury surveillance	N/A	Required access	Requires annual medical physicals and accident reviews and recordkeeping. Allows for medical information to be used in certifying benefits but data provisions are vague
Virginia					
Alexandria and IAFF 2141 (2023-2026)	Presumed, mandated, permissive	Injury surveillance	N/A	Limited access, required reporting, required employee access	Requires exposure recordkeeping, injury reports, and authorizes broad electronic monitoring. Allows for voluntary disclosure of injury or fatality to the union. Requires employee access to exposure records
Arlington and IAFF 2800 (2023-2026)	Mandated, restrictive, permissive	Anti-discrimination, benefits, injury surveillance	Location, duration	Limited access, required reporting, required employee access	Allows for collection and maintenance of injury, fatality, illness, accident, and exposure information. Authorizes electronic monitoring for health and safety purposes but does not address storage or access/sharing for this data

Notes: "Restrictive" policies limit collection of data. "Permissive" policies allow data collection. "Presumed" indicates that the policies do not explicitly address data collection, but presume it has or will take place. "Mandated" requires data collection.

Chapter Three (Manuscript Two): Data in the fire service: firefighter and fire service leadership perspectives on current practices, challenges, and gaps

Abstract

Objective: There is growing interest in utilizing firefighter health and safety data to understand and prevent illness, injury, and fatality. However, there is little evidence on firefighter or leadership data privacy preferences. We examined fire service stakeholder perceptions of current data practices.

Methods: We conducted interviews and focus groups with career firefighters in Maryland and Virginia; interviews with union representatives and department-level leaders in each state; and interviews with national-level fire service leaders (March – November 2023). Interviews and focus groups were audio recorded and transcribed. We analyzed transcripts using thematic analysis.

Results: We conducted 35 interviews and 4 focus groups (65 total participants). The sample included 31 career firefighters, 2 union leaders, 11 national leaders, and 21 department-level leaders. We identified 13 themes across 4 categories. Fire departments collected a range of health, injury, and exposure information to establish firefighter fitness for duty, help firefighters obtain benefits, conduct prevention, and advance administrative priorities. Firefighters had few data privacy concerns but generally favored data deidentification and aggregation. Leaders described pushback from firefighters related to concerns about job repercussions and privacy

and described cultural and resource limitations. Firefighters and leaders desired more mental health and exposure data. Leaders called for improved data infrastructure and firefighters wanted better data communication.

Conclusions: Firefighters and leaders viewed data as a tool for advancing health and safety but identified barriers to data collection and use. Participants identified priorities for future data collection and the need for resource investments, cultural shifts, and enhanced data communication and protections.

Introduction

Firefighters take on great personal risk to provide essential services for their communities. There are approximately 1 million firefighters in the United States who respond to over 25 million calls each year.[112,113] Firefighters encounter a vast array of incidents, including fires, natural disasters, and medical emergencies requiring emergency medical services (EMS).[113] Firefighters sustain high rates of injury and fatality in the line of duty: in 2022, there were over 65,000 on duty injuries and 96 on duty fatalities.[1,2] Beyond these on duty incidents, firefighting has been linked to a host of long term adverse health outcomes, including elevated rates of certain cancers.[46,47] Firefighters are highly attuned to the risks of their profession, and have emphasized concerns related to high rates of injury, cardiovascular disease, mental health challenges, and cancer.[114]

There are growing calls to utilize firefighter health and safety data to better understand the hazards of firefighting and design interventions to protect future generations. This could include data from national injury or disease registries, biometric data from wearable devices, exposure data, or self-reported risk factors associated with diseases such as cancer.[3,55,56,115] Many new data collection efforts are focused on the national level, through national-level injury surveillance and research.[3,52] Researchers have identified serious flaws in existing data infrastructure, such as large swaths of missing occupational data in cancer and burn registries, and highlight the need for more sophisticated data reporting and data linkages.[50–52] In light of these structural challenges, government agencies have begun to invest in infrastructure to support firefighter injury surveillance and health research. In 2023, the National Fire

Administration announced that it would transition its legacy incident reporting system, the National Fire Incident Reporting System (NFIRS), to a modernized analytics platform, the National Emergency Response Information System (NERIS). Fire departments currently report incidents to NFIRS, although participation is voluntary and it documents only 70% of the overall incidents that occur each year.[116] NFIRS, which includes a module for firefighter casualties, requires in depth manual data entry.[117,118] NERIS, which is currently in development, will be cloud-based and support data linkages and a range of new data collection, including sensor data and biometrics.[54,118] From a research standpoint, the National Institute for Occupational Safety and Health (NIOSH) recently launched the National Firefighter Registry for Cancer, which will link firefighter cancer diagnoses to state cancer registries.[53]

While these efforts hold promise for improving health and safety nationwide, little is known about how fire departments are collecting, using, or sharing firefighter health and safety data. On a local level, departments are well positioned to collect data on their workforces and to use this data to design and implement tailored interventions to reduce injuries and fatalities. There are a wide array of products for departments to track injuries or exposures, and growing calls for departments to leverage data.[119,120] However, to our knowledge, there are no studies assessing the state of current data collection in fire departments, including perceptions of whether such data is adequate and the challenges associated with collecting and managing data on an organizational level.

More broadly, expanding the collection of or access to firefighter health and safety data at any level raises concerns about data privacy.[3] Additional firefighter data might help improve health and safety, but collecting this data, particularly within fire departments, raises concerns about data privacy, as firefighters might be asked to share sensitive health information with their employers, government agencies, or researchers. There is little research on data privacy in the fire service, and existing studies tend to focus on the acceptance of new technology within fire departments. One study examining the implementation of a biometric device concluded that firefighters are concerned about the impact of technology on their autonomy and that firefighters were more skeptical than department leaders.[59] Another study assessing the factors impacting perceptions of a biometric device identified concerns related to workplace accountability, data access, and employer trust.[58] However, no studies to date have assessed current data collection, use, and sharing practices within the fire service, and the acceptability of these practices among fire service stakeholders. This hinders our ability to understand the kinds of data collection firefighters support and areas where leadership see urgent needs to strengthen the fire service's data efforts.

This study examines perceptions of current occupational health and safety data collection practices among firefighters who might be asked to provide such data, and departmental and national leaders who might collect, access, or use such data. Our findings identify challenges for current data efforts and opportunities to ensure the ethical implementation of new data initiatives.

Methods

This is an exploratory study examining fire service stakeholders' perspectives on data privacy topics. Because there is limited evidence on this topic and we wanted to understand a wide range of potential views and motivations, we opted for qualitative methods to explore attitudes towards firefighter data privacy. We conducted a combination of semi-structured interviews and focus groups to understand fire service stakeholders' perspectives on current data practices.

Sample and recruitment

We identified three subgroups that we anticipated would have distinct views towards data in the fire service: career (sometimes referred to as "paid") firefighters, department leaders, and national-level fire service leaders. For career firefighters and department leaders, we first sampled departments, as we wanted to recruit firefighters and leaders within the same department to enable comparisons. A member of the study team has experience working with fire departments to develop the Firefighter Organizational Culture of Safety (FOCUS) survey, which is now used in practice settings to assess fire department safety culture.[121] We sampled fire departments that had previously or were currently participating in FOCUS surveys in Maryland and Virginia, recruiting two departments in each state (four departments in total). Because we were interested in occupational health and safety data, in which firefighters might be sharing personal information in an employment context, departments had to be staffed by career or mostly career firefighters to be eligible.

Within each fire department, we worked with a point of contact to recruit career, rank-and-file firefighters to participate in focus groups. In a Maryland department where we were unable to recruit sufficient participants for a focus group, we conducted a semi-structured interview. To understand the role of unions in representing firefighters' interests, we also recruited union leaders in participating departments. For each department that was unionized, we invited union leaders to participate in semi-structured interviews.

To recruit leadership participants within fire departments, we worked with a point of contact to identify individuals in overall leadership, health and safety positions, or in human resources (HR) positions. We recruited both sworn members of the fire service and civilians (e.g. non-firefighters working in leadership in departments or fire service organizations) to participate in semi-structured leadership interviews. We included both sworn members and civilians to capture a wider range of perspectives and because in all participating departments, the individuals serving in relevant roles (e.g. health and safety) included both civilians and firefighters. At the national level, we used purposeful sampling to identify participants in government, advocacy, and research organizations. Participants had to be affiliated with a fire service entity within one of these three categories (career firefighters, fire department leaders, or national fire service leaders) to be eligible to participate. For the leadership subgroups, we also conducted snowball sampling and asked participants to recommend potential participants in their professional networks.

Data collection

We sought participants' views towards current data practices with regards to three fundamental aspects of data privacy: data collection, data use, and data sharing or access. We focused on these three domains because they are all important elements constituting data privacy preferences.[27] To facilitate comparisons across subgroups, we asked all participants about their views within these domains, but modified the questions slightly to recognize their different roles. We asked all participants demographic questions; for focus group participants, we asked them to complete an exit survey at the end of the group to protect their confidentiality. Appendices 3.1-3.5 contain questions from the interview guides, the focus group discussion guide, and the exit survey.

Data collection took place from March – November 2023. All interviews were conducted over Zoom and all focus groups were conducted in person at fire stations. In the two Virginia departments, focus groups were held at fire stations while firefighters were on duty. In some groups, firefighters were taken out of service for the duration of the group, meaning that they were not responding to calls. In other groups, participants were in service and if they received a call during the group it was briefly paused or continued with the remaining participants until the full group rejoined.

Following each interview or focus group the interviewer wrote memos to summarize the discussion, reflect on themes, and document initial observations.[122] We obtained oral consent and audio recorded the interviews and focus groups. Recordings were transcribed verbatim

using a professional transcription service. This research was approved by the Johns Hopkins Bloomberg School of Public Health Institutional Review Board.

Analysis

We conducted data analysis in an iterative fashion using thematic analysis.[122] One team member developed a codebook based on the memos and interview/discussion guides. A second team member reviewed the codebook after reading memos and transcripts. Both team members coded an initial subset of transcripts and met to compare coding and resolve disagreements. After revising the codebook and double coding additional transcripts, the team members independently coded the remainder of the transcripts, meeting to discuss questions about code application as needed. The codebook is included in Appendix 3.6. Coding was conducted in Dedoose.[123]

We categorized participants into two overall groups for analysis: firefighters (rank-and-file firefighters and union leaders) and leadership (department leaders, government officials, advocates, and researchers). We present our findings primarily in terms of these two groups, as the subgroups within each are conceptually similar and we found similarities in views within each group. For instance, the union leaders we spoke to were themselves career firefighters not in department leadership positions. And while some advocates represent firefighters' interests, in many cases they have unique, national-level views on data privacy topics given their roles. In describing our results, we differentiate between subgroups when relevant and note when participants held multiple roles, such as Fire Chief and Advocate.

Results

Sample

We conducted 35 interviews and 4 focus groups of 5-9 participants each with a total of 65 participants. Our sample included 31 career firefighters, 2 union leaders, 11 national leaders, and 21 department-level leaders. Table 3.1 shows participant breakdown by role and jurisdiction. Our firefighter sample is weighted towards VA, with 30 VA firefighters and 1 MD firefighter, due to data collection challenges in MD.

Our sample was predominately male and white, consistent with the overall demographics of the fire service.[60] Leadership participants included more women (34%) compared to firefighter participants (12%), and more racial diversity (25% non-white compared to 9%). Leadership participants were older than firefighter participants (mean age of 48 years compared to 36 years) and more experienced (mean of 12 years compared to 25 years). Table 3.2 shows participant characteristics across subgroup. Focus groups lasted an average of 77 minutes. Firefighter interviews were an average of 39 minutes, and leadership interviews were completed in an average of 45 minutes.

Themes

We identified 13 themes within 4 categories: 1) current data practices, 2) the value of data in the fire service, 3) data challenges, and 4) priorities for addressing gaps in current practices.

Table 3.3 shows the themes in each category and an overview of themes by stakeholder group (firefighters and leadership).

Current data practices

Participants' descriptions of current data practices within their organizations included the kinds of data collected, and data access, sharing, and reporting practices.

Kinds of data collected

Leaders and firefighters within the same departments provided consistent descriptions of the kinds of firefighter health and safety information collected, although data collection varied across departments. All departments collected information related to firefighter injuries, exposure to occupational hazards, vital signs on a fireground, and regular physical exams. Injury reporting was fairly standardized across jurisdiction, with departments collecting information about the nature and cause of injury. In contrast, exposure documentation varied. Some departments focused on exposures sustained during EMS calls such as blood borne pathogen exposure from a needle stick. Others documented fire-related exposures if an event was perceived as particularly hazardous. A few leaders also described requirements for documenting hazmat exposures. All departments collected vital signs such as heart rate and blood pressure on a fireground (referred to as "rehab"). The frequency and thoroughness of annual physicals and frequency varied by department, with some conducting in-depth National Fire Protection Association (NFPA) 1582 physicals, as dictated by a fire service standards organization, and

others requiring a civilian physical. Three departments conducted regular fitness tests, with varying degrees of intensity.

Several department leaders and firefighters suggested that in some cases, departments intentionally avoided collecting or documenting sensitive information related to physical or mental health. For instance, most firefighters stated that there is no documentation of peer mental health support services and most departments did not receive members' annual physical results, other than learning if they passed or failed. Participants framed this approach as an effort to protect individual privacy and encourage firefighters to utilize services. A few explained that firefighters were less likely to access peer support services if they thought such a request would be documented.

National-level leaders described a range of data collection conducted by their organizations. Government officials described routine collection of firefighter injury surveillance data, and researchers collected a range of injury and exposure information related to their work. For the most part, advocates did not directly obtain firefighter occupational health and safety data, although a few organizations helped facilitate research. Several advocacy participants discussed research partnerships to examine issues impacting underrepresented minorities in the fire service, such as rates of harassment or discrimination, or health outcomes specific to female firefighters.

Data access, sharing, and reporting practices

Within departments, firefighters and leadership described limited internal sharing of firefighter health and safety data, and most believed that such data was adequately protected by their departments. Nearly all leaders indicated that access to identifiable firefighter health or safety information was granted on a need-to-know basis with relevant personnel. For instance, injury information was accessible only to health and safety staff.

Several leaders also emphasized the importance of ensuring that individuals had access to their own data, such as their annual physical or fitness exam results, both because it was the right thing to do and because it might empower firefighters to make healthy choices. While identifiable data was closely held, aggregated data sharing was encouraged by many department leaders who supported sharing results such as department injury trends to enhance prevention activities. And while these protocols and confidentiality might be formally upheld, many firefighters and a few leaders noted that news about physical injuries traveled fast.

> Just like with the injury thing, you can decipher who's, we heard, oh, such and such went to the, whatever that thing is in [State], the mental health rehab center. Oh, this guy's on injury leave for the next three months. Wonder where he is. We can find out things by digging. – Firefighter

Externally, department leaders reported injuries to a range of organizations including government agencies like OSHA and third parties like NFPA and the International Association of Fire Fighters (IAFF) union. Firefighters were less certain about how data might be reported externally, but assumed that injury information was shared with government agencies or third parties. Government leaders and researchers described efforts to keep identifiable information

secure while supporting widespread sharing of aggregated and deidentified results for educational purposes. While most advocacy organizations did not collect extensive health or safety data, they endorsed returning individual data to firefighters and publication of trends.

Value of data in the fire service

Participants described four use cases for firefighter data: establishing fitness for duty, helping firefighters obtain benefits, conducting health and safety prevention initiatives, and advancing administrative priorities.

Establishing fitness for duty

Within departments, both firefighters and leaders depicted medical and fitness information as being used to establish fitness for duty status. All departments used regular physical exams to determine if a firefighter was fit to perform their job; in cases where a firefighter did not pass a physical, they might be placed on light duty, performing limited job tasks, or be offered additional training. Some departments also required an annual fitness exam to evaluate fitness for duty, whereas in other departments fitness assessments were optional for some personnel or the results were not punitive (e.g. if an individual did not pass, they could continue in their role). In departments where fitness assessments were optional or non-punitive, the exams were aimed at providing individual firefighters with insights on their fitness. Some leaders in these departments stated that firefighters who did not pass fitness assessments were offered optional fitness training programs.

Obtaining benefits

Participants across all stakeholder groups cited injury and exposure data as a tool for helping firefighters obtain workers compensation or presumptive benefits to care for occupational injury or illness. Firefighters discussed this repeatedly, highlighting the importance of documenting injuries, even if minor, in the event that they needed evidence to prove an injury was work related. Although most firefighters described an antagonistic relationship with workers compensation, in which they believed claims were denied even with supporting evidence, they still believed documenting injuries was important. Two firefighters described the process:

> Participant 9: It's kind of a pain and it's valuable kind of. [laughter]
> Participant 5: Well, I feel like it's only valuable if you do something about it right then. If you do something like if I say, I felt a pain in my knee and then three months later you have an injury off duty. Let's say, well, there's no way that we can positively tie it back to that. Worker's comp isn't going to cover it. – Firefighters

Firefighters also noted that exposure documentation was increasingly essential for obtaining disability and retirement benefits, particularly for occupational cancers, which are a growing concern in the fire service. Firefighters and leaders noted that despite presumptive benefit laws, which establish a list of cancers which can be "presumed" to be work-related for firefighters, many firefighters need extensive documentation to establish an occupational cause of these diseases. A firefighter said:

> I think you see that [exposure documentation] more with prevalence of like cancers and stuff. Because it's like, I mean, they have like presumptive acts but still you kind of have to prove it still. So, having the [exposure] forms definitely are beneficial moving forward. – Firefighter

Some firefighters and advocates noted that claims could be denied even with extensive documentation. An advocate believed that exposure data could be used against firefighters, pointing out that some presumptive benefit laws require evidence that a firefighter was exposed to occupational hazards within a certain time frame. If a firefighter lacked this documentation or was exposed just outside of the required time frame, this might disqualify him or her from receiving benefits. Despite these concerns, firefighters and advocates believed that it was still beneficial to record exposures.

Conducting health and safety prevention

Leadership participants were enthusiastic about using injury, fitness, and health data for prevention. Several departments had health and safety personnel and/or committees that used injury and fitness data to understand trends within their departments and design interventions. Participants broadly agreed that the intent of health and safety staff was to understand and reduce injuries , although there were mixed views within and across departments about whether these injury prevention efforts were effective. One leader explained:

> So, on a departmental level, we use [injury and exposure information] to track trends and identify. We can use, if we have a bunch of people getting exposed to similar things, then that's a safety program focus. Or if we have injuries that are occurring in the same way, obviously there's probably some engineering controls that we can put in to reduce those injuries. – Department Leader

Government officials described using injury reporting data to conduct injury epidemiology studies and uncover underlying causes of injury and fatality. Advocates who were not necessarily directly involved in injury data collection or analysis expressed support for health and safety research using injury and fatality information. A small number of leaders both in

advocacy and departmental roles highlighted research studies that examined the health and safety of underrepresented minorities:

> . . . one of the areas we're focused on is diversity, equity and inclusion, and identifying some of the reasons why different demographics maybe have higher cancer rates, or are not getting cancer screenings more regularly or when they should . . . We're really seeing that our Black members are having significantly higher specific cancer rates, and that's something where in our department, we can really push for some of the – Like the educational efforts really highlight that and why is that. – Advocate

In a few rare instances, firefighters acknowledged that injury data was used by health and safety workgroups or discussed annual medical or fitness exams in terms of keeping personnel fit. However, for the most part firefighters did not discuss preventive applications for health and safety data.

Supporting administrative priorities

Leaders characterized data as a tool for achieving administrative priorities like obtaining funding, improving recruitment and retention, and enacting policy changes. Individuals in departments, advocacy organizations, and government described using data to justify expenses like new equipment, hiring new personnel, or to link reductions in workers compensation expenses to injury prevention efforts. While they focused on the financial outcomes, many leaders' comments were ultimately aimed at securing funding to protect firefighters. One department leader simply stated:

> I mean, I need the data to explain why I need money. Ultimately my job is to get money to buy my firefighters stuff to protect them, to take care of them. – Department Leader

A smaller number of department and advocacy leaders described the power of evidence to help advocate for policy change. These individuals emphasized the need for research to inform National Fire Protection Association or federal policies, or to change department policies.

Challenges

Participants described a range of factors that either facilitated or hindered high quality data collection, use, and sharing. These included resource and logistical challenges, cultural and communications factors, data considerations, and fears about job repercussions.

Resource and logistical challenges

On an individual level, participants across stakeholder groups described challenges in collecting accurate and complete firefighter data. Firefighters primarily focused on administrative burdens of completing injury and exposure paperwork, which they viewed as time consuming and annoying. One firefighter said:

> Don't get hurt. It's easier. Because it is -- I mean, [injury reporting] it's like anything else. It's extra. You don't want to do it. Like it's aggravating. – Firefighter

These frustrations were magnified by the perception that even after completing paperwork, their claims for workers compensation could be denied. Most firefighters viewed exposure documentation as more burdensome than injury reporting. Some acknowledged that completing exposure documentation might help them obtain coverage in the future, but many stated that they do not keep comprehensive logs of their exposures, largely due to the administrative burden. Leaders in departments, advocacy, and research agreed that it is difficult

to collect high quality firefighter data, noting that this documentation burdens an already taxed workforce.

On a department level, nearly all leaders described challenges in collecting or analyzing existing data because of time, personnel, or funding limitations. Several participants noted that they simply lack the personnel or funding to conduct serious data collection or analysis. One leader explained:

> For our department, it is lack of resources. Human capital and then technology. We're still working out of Microsoft Office products . . . I think the barriers are really fiscal. – Department Leader

In other cases, leaders believed that they could access desired data, but simply lacked the expertise, time, or software to use it. Two departments lacked software for injury documentation and analysis, and were using a combination of paper forms and Excel. Departments also had difficulty linking datasets within their jurisdictions (e.g. with risk management) and aggregating data. Participants believed these challenges prevented them from being able to see trends, understand their causes, and react accordingly.

On the national level, government, research, and advocacy stakeholders all expressed frustrations about a lack of data linkages in the fire service. Several pointed out that this prevented data access from sources such as researchers, or increases administrative burdens on departments by requiring reporting to multiple sources. Some also described technical limitations of existing systems used to collect data, such as the National Fire Incident Reporting System (NFIRS).

Cultural factors

Leaders were also highly attuned to cultural factors that were influential in collecting and using firefighter data. Several participants were concerned about general apathy towards data in the fire service. Within departments, many leaders depicted their organization's posture towards data as outdated, and a few were critical of their departments' data initiatives, describing them as lackluster. More generally, national and department leaders suggested that the fire service as a whole did not value or prioritize data; many attributed this stance towards a culture that prizes tradition and is resistant to change. One department leader said:

> But as a culture, the fire service, we've been doing the same thing since we started, whether it's fire, rescue, or medical. The people aren't changing, they're just getting more of them and more of them. So, I think it would be a good push to move data collection, data utilization, and then policy changes to help move the entire industry forward. – Firefighter (serving in leadership at headquarters)

Firefighters did not raise these types of industry-wide concerns, and did not express opinions about their departments' culture towards data.

Data considerations

For the most part, firefighters appeared comfortable with the level of information that they shared with their departments, as well as how this information was disseminated among department leadership. Some simply did not express strong views on current practices, whereas others believed that efforts to limit sharing were sufficient. Others stated that sharing personal information related to their physical health simply came with working in a high-risk, public job.

> I don't have any real experiences or bad or positive experiences with my data in the department, except for just our health as in our yearly physicals and then stress tests and things like that. And I haven't had any issues with those or anything. – Firefighter

> I'm sure no one loves to give all their personal information to an employer, but it's probably necessary in this particular field… – Firefighter

In a few cases, participants described instances in which their departments were proactive or responsive to concerns about privacy. For instance, one department switched from sending medical exams through interoffice mail to individuals' homes, and another stopped posting public lists of personnel whose physicals indicated they needed follow up stress tests. Although a few individuals were troubled by how quickly news about health diagnoses or injuries could spread in their departments, they pointed out that this typically occurred through informal channels in which firefighters share information with each other.

Although most firefighters were comfortable with current practices, some expressed preferences regarding how their information might be shared. Many had a general preference for limiting the sharing of identifiable information and opting for aggregated data sharing both within or outside of departments, on ideological grounds. Union representatives shared this view and argued for the use of aggregated data whenever possible. Union leaders also identified a broader resistance to sharing medical information, in part based on individual privacy preferences, but this concern did not arise in focus group discussions.

In a few instances, firefighters expressed distrust in government, particularly federal institutions, although no one voiced these concerns when discussing reporting of injury information to

NIOSH or OSHA. Firefighters were broadly supportive of sharing information with researchers conducting health and safety research, although some described their frustration that they did not receive their individual results or the overall results of studies in which they participated.

Reluctance to sharing identifiable information appeared to be heightened based on the sensitivity of the data in question. One female firefighter pointed out that she viewed reproductive health information as more private than physical injury information. Firefighters generally agreed that mental health information was closely held, including among peer networks. In one focus group, firefighters described their dismay when asked to complete a mental health research survey that was theoretically anonymous, but asked for information like station and years of service, which participants believed could be used to identify them. Firefighters explained their reasoning behind not wanting to share information:

> Participant 5: I'm not worried about being a target for anything other than I don't want -- I would rather my personal information not released outside the organization that I'm tied to . . . It's just too many easy ways for people to get access to me, which gets access to my family, the way I feel about it.
> Participant 4: Well, but that survey we just did, it has a lot of pretty in-depth. If you take it seriously, it has a lot of in-depth personal mental health. Like, for example, I think there's some on there like, have you ever considered committing suicide? Like, how many times in the last week have you felt like, that you were too depressed to come to work? So just there's different. And at that point it's just kind of like...eh…
> Participant 3: And you don't know where it's going.
> Participant 4: You don't know where it's going.
> Many: Yeah.
> Participant 4: Then you get to the end. It's like basically you got to describe your eye color, you know. [laughter] – Firefighters

Leadership's views were largely consistent with firefighters. They were aligned with firefighters' in preferring that data be deidentified and/or aggregated for research and prevention. Some

leaders thought that firefighters were less likely to share information if they believed it would be identifiable:

> Even if you tell them it's going to nobody but me or nobody but this specific office, they are less likely to participate if there is identifying information. – Department Leader

Leadership identified additional factors that they believed influenced willingness to share health and safety information. For instance, several department leaders stressed that health and safety data should be used in non-punitive ways and described efforts to convey this to members:

> I mean, certainly, you know, we're not going to use injury data for discipline or anything like that. That's a big concern . . . we try really hard in our office, at least the safety office, that we are not a punitive type of section of the department. Because once we become punitive, people stop talking to us. People stop trusting us. And our job is to try to make things safer for them. And we can't make things safer if we don't really truly understand what the problems are, you know? – Department Leader

Others indicated that firefighters were more reluctant to share mental or behavioral health information due to fear of reprisal and/or the sensitive nature of this data. A few department leaders also described generalized firefighter pushback towards mandatory collection of fitness information.

Some research and advocacy participants thought that firefighters would be more likely to share information with external entities (e.g. researchers) than within their departments. Although most firefighters endorsed research, these comments were oriented as support for research initiatives as opposed to a broader preference for limiting data sharing within departments. There were mixed views among leaders about whether or not firefighters were ideologically

opposed to sharing data within departments, with some leaders describing widespread privacy concerns, and others believing that such views were rare. A few national leaders also discussed the use of informed consent to gain buy in for research, and promoted providing individual access to one's own data as an incentive for sharing information.

Beyond individual-level data collection and sharing, a small number of leaders highlighted structural challenges that hinder data access and utilization in the fire service. One government official pointed out that comprehensive injury databases exist, but they are held by workers compensation insurers, and inaccessible for public use or research purposes. A few department and research participants described challenges in securely storing data, which prevented data collection entirely or limited the kinds of data that could be collected. These participants discussed the tension between using data to advance health and safety priorities while respecting individual privacy rights. Finally, a few leaders raised questions about the subjectivity of data, questioning if data could be analyzed without bias or arguing that data could be twisted to align with any viewpoint.

Job repercussion fears

Leaders across all subgroups, as well as union representatives, believed that firefighters were fearful that sharing health or injury information could result in job loss, changes in job status, or impact their identities as firefighters. Many described encountering concerns among some firefighters that if they did not pass medical or fitness exams, they would be terminated. Most

department leaders believed these views were unfounded and expressed a desire to use these exams for health and safety purposes:

> Because you have firefighters that will be like, “a machine or a doctor or this METS [metabolic equivalents] does not dictate on how I can fight fire”, which is true . . . [but] all the research they've done with this, says that if your METS are below eight, you are at a higher risk of dying of an MI [myocardial infarction] or something out on fire scene. So that's the biggest issue I feel in the fire service. Everyone thinks that we're trying to take their job away or take a ton of money out of their pocket, what they don't understand is, no, we're trying to keep you healthy and safe and everything like that. – Department Leader

Only one leader suggested using health or safety data in punitive or disciplinary ways, arguing that it was difficult to emphasize prevention if there was no accountability for lack of fitness.

In other cases, leaders anticipated firefighter concerns that sharing health information would result in changes to job status, affecting day-to-day work even if employment status and pay remained unchanged:

> I know a couple cases [of] people that never reported anything because they didn't want to go through the process. Because you got to go to the county clinic and then you got go to the headquarters, and most people get into this job for adrenaline rush and helping people. And then you're on modified duty, sitting behind a desk with limitations. – Department Leader

Several individuals framed these concerns as fears about losing identity as a firefighter:

> Their fear isn’t so much losing their job, their fear is losing their identity, who they are. – Advocate/Department Leader

While these concerns were widespread among leaders, most firefighters did not discuss job impacts. A few were worried that their annual physicals had become so in depth that they might identify health risks for which they are terminated or moved to light duty, although this

perspective arose in only one group. One firefighter framed hesitation about sharing physical, and especially mental, health information as concern about losing trust among colleagues. Union leaders attributed hesitation about sharing medical information to underlying concerns about fitness for duty and privacy, but were still supportive of annual exams and believed they helped maintain their members' fitness for duty.

Priorities for addressing gaps in current practices

Participants identified three areas where they would like to see improvements in existing data practices: new data collection, strengthening data infrastructure, and improving data communication.

New data collection

While some participants did not see any gaps in existing data practices, most described a wide array of areas where they believed additional data would enhance the use cases they articulated for existing data. Firefighters and leaders agreed on several priorities, but leaders identified a more extensive list of gaps.

There was widespread support for collecting more data on individual firefighters' exposures to help facilitate benefits. For instance, firefighters and leaders suggested that documenting every exposure to a fire scene would provide firefighters with evidence that potential illnesses were work-related:

> Participant 8: I think what [Participant 5] said earlier, the exposure thing would be great if we could do probably more of that. Because everything we do now is tied to cancer. Everything we do. Even down to what we wear is proven to cause cancer.
> Participant 3: To speak on the exposure stuff. I know you were talking about the NFORS app or the NFIRS program. I just recently came from another locality and in our NFIRS that…we documented every fire that we went to as an exposure so that it was the officer or the driver's job to make sure that everybody was put in. Which as I'm learning here now, that doesn't happen on every call. So yeah, it would be nice that on every one, because you never know how long or when [presumptive] laws change. – Firefighters

Both leaders and firefighters highlighted the need for additional mental health data. Although mental health was not mentioned in all discussions, there was a general consensus among participants that the fire service was trying to heighten attention on and services for mental health. A few leadership participants specifically called for more data collection, with one department leader arguing for an annual mental/behavioral health exam. Similar to an annual physical exam, he indicated that the department would be interested only in fitness for duty status, not the full individual results. In a focus group in this department, participants suggested and strongly supported an annual mental health evaluation that could both offer services and serve as a fitness for duty evaluation.

Leaders of all kinds argued for more data on nonfatal injuries to better understand and prevent adverse events. Participants called for expanding the evidence base on the causes of injury, associated health risks or characteristics, and specific injury trends such as rising rates of violence against first responders. A small number of participants advocated for collecting additional health or medical information from physicals or on a fireground. Some also noted

rising awareness about occupational cancers and called for cancer research, with almost all emphasizing the need for a basic understanding of cancer rates. One leader explained:

> I know I can't have personal data on the medical information, but I'd like to know how many heart attacks we've had in this fire department. I'd like to know how many cancer cases we've had in this fire department. Because then that will help me go to bat for more cardiac programs, more prevention programs on this. – Department Leader

Many department leaders desired more fitness information, including general fitness statistics, an incumbent fitness exam (in departments where this did not already exist), or exercise logs. Leadership believed that a better understanding of their members' fitness would allow them to pinpoint areas of weakness across the department and implement training programs, ensuring their workforce was both fit for duty and healthy. A small number of firefighters in one focus group shared this view and criticized existing fitness exams as insufficient for capturing fitness for duty. A few leaders in departments and research organizations also called for biometric information from fitness devices or wearable devices worn on a fireground.

A small number of participants, largely in advocacy and senior leadership positions in departments, saw a need for more data on the experiences of underrepresented minorities in the fire service. Advocates called for collecting demographic and retention information to establish baseline statistics on representation and discrimination against women and racial minorities. Others called for additional research on the impacts of firefighting on women's reproductive health, both for prevention and to increase the evidence base for presumptive cancer policies. While our sample included few female firefighters, one female participant noted that the lack of evidence on female firefighters has far reaching impacts:

> I can remember sitting and having a discussion with a bunch of the ladies I work with that, oh, we tend to have more shoulder injuries because they set up the cabinets in the apparatus for somebody who's six two, not somebody who's five four. Things like that. We work a lot more overhead. And I don't know how much in the department they're looking at age, height, gender specific, how they're sorting that data as far as looking at it. That's been one of my pet peeves when it comes to safety equipment. I was just joking yesterday, it's my dream that before I retire, I actually have boots and gloves that fit me. [laughs] – Firefighter

Strengthening data infrastructure

Several leaders noted that even if data was theoretically available to them, they encountered challenges accessing or utilizing information. For instance, some individuals noted that injury data was already collected by various entities but reporting varied for different organizations and there were no data linkages. Leaders from all departments desired better technology to assist with collecting or analyzing their health and injury data:

> We have access to most of the stuff that we need. What we don't have currently is a way to really look at that and a way to really aggregate that . . . we have not really found a product out there that has fulfilled our need for this. And really kind of gives us a snapshot at root causes. – Department Leader

Examples of desired technology ranged from software to track injuries to sophisticated wearable devices or live dashboards that could be used on firegrounds. While firefighters were less attuned to the technological infrastructure that might enable new data collection, a few noted that automating data collection could help document exposures (e.g. if the call system automatically documented who responded to a fire call).

Improving data communication

Department leaders and advocates highlighted the importance of partnering with trusted leaders such as union officials, and communicating well about the purpose of data collection. A small number described challenges in sharing data effectively, pointing out that sharing incomplete data could have harmful effects, and noting the difficulty of communicating nuance.

Advocates and firefighters highlighted the need for better data interpretation and dissemination. Several firefighters wanted more information about the purpose behind data collection efforts or the interpretation of their individual results. For instance, some described not knowing how to interpret annual physical test results:

> I'm going to voice off. I think the value sucks, to be honest. They do blood work and they do a full physical but nine times out of 10 we get a paper back that says, hey, there was something abnormal about your blood work or something we found, and that's it. No follow up, no telling you what it actually is. And to actually follow up with them to find out is really hard. They do the work, but they don't actually give you the results. – Firefighter

Others were frustrated with the lack of research results described earlier. The lack of communication about their own data and/or study results led them to conclude that a large share of data collection has no purpose or no ultimate benefit to firefighters.

> Participant 2: Well look at the urine samples that they would collect, stuff like that. They had us give a urine sample after we got back from fires to see, hey, do you have whatever…
> Participant 9: This has been absorbed into your bloodstream.
> Participant 2: Arsenic, you know, absorbed into your body.
> Participant 3: We did it for two years and got…
> Participant 5: And they lost funding and...
> Participant 2: Right. They lost funding and it went away. Or every sample you gave, you got zero back from…
> Participant 5: No idea. – Firefighters

Discussion

This study examined current data practices in the fire service and firefighter and leadership perspectives on the benefits, challenges, and shortcomings of existing data efforts. Our findings confirm that department-level leaders and firefighters are generally supportive of research and governmental efforts to expand data collection.[52–54,120] Participants highlighted the value of existing data and opportunities for the fire service to strengthen its data capabilities in pursuit of a healthier and safer workforce. Although participants sometimes characterized data as a challenging or complicated asset, overall we found that data was highly valued. Fire departments in our sample collected a similar range of health and safety data. While there were some differences in the level of detail or manner in which it was collected, we found that departments were aligned in trying to document health or exposure information to benefit firefighters. Nearly all leadership participants viewed data as a powerful but underutilized tool for helping keep firefighters fit for duty, healthy, and safe. And while firefighters identified a smaller range of use cases, they noted the potential for data to aid them on an individual level when filing for benefits.

Many leadership and firefighter participants identified the need for additional exposure and mental health data collection. This is consistent with calls for research on cancer and mental health in the fire service, and a study that identified these issues as major health concerns among firefighters.[46,114,125–127] Our findings confirm the need for additional data on these topics and identify specific kinds of data that would be helpful, including but not limited to data used for research purposes. For instance, firefighters described a need for extensive documentation

of exposures so that if they developed cancer, they could link it to their occupation. While presumptive laws should help firefighters receive coverage for occupational cancers, participants in our sample described the need for vast amounts of exposure data that they often did not have. Collecting exposure information through departments or third party organizations (e.g. exposure mobile applications[119]) would help ensure that firefighters are well equipped to receive coverage in the event that they are diagnosed with cancer.

Firefighters' descriptions of the value of exposure data also reflect a potential disconnect between the purpose of presumptive benefit laws and the burdens firefighters face in filing for these benefits. Presumptive benefit laws are designed to facilitate coverage for occupational diseases by designating specific conditions that are presumed to be occupational.[128,129] While these laws are intended to ease the process of filing for coverage, firefighters in our sample indicated that they still require significant documentation of exposures that firefighters may not have at their disposal. Future reforms to these laws should account for the availability of exposure data. It will be difficult for these laws to facilitate benefits if firefighters do not have detailed exposure records and it is burdensome for them to create or maintain records.

Our findings also offer insights on how fire departments might begin to evaluate their firefighters' mental health. Researchers and national leaders have called for research on the impacts of firefighting on mental health outcomes, and identified a need for department-level interventions alongside national-level surveillance to assess mental health risks and prevent suicide.[125,127,130,131] Firefighters and leaders in our sample argued for additional mental health

data collection within fire departments, both to evaluate fitness for duty and to ensure that firefighters could be connected to services. This suggests that there is enthusiasm for department-level mental health assessments, but also raises questions about how to ethically implement mental health interventions in occupational settings. While mental health screening could provide important supports, it raises serious data privacy concerns, especially in light of our finding that mental health information is viewed as highly sensitive. Future research should examine the acceptability of various mental health screening models and firefighters' preferred modes for receiving mental health supports.

While only a small portion of our sample discussed using data to understand the experiences of women and racial minorities, there are significant opportunities to collect data in support of a more diverse and inclusive fire service. Participants called for data to help understand recruitment and retention trends and health and safety outcomes specific to underrepresented minorities. Researchers have begun to examine outcomes specific to women in the fire service—for example, fitness, tobacco and alcohol use, reproductive health (e.g. rates of miscarriage), and harassment.[132–135] Departments and researchers should build upon this work to examine recruitment and retention trends, assessing whether women or racial minorities have differential experiences in the recruitment pipeline, and why they leave the profession. Researchers can also examine additional health and safety outcomes specific to underrepresented minorities. Researchers, as well as some leaders in our sample, noted that the small sample size of women in the fire service often leads to their exclusion from studies.[132]

Future work should specifically examine how female firefighters perceive their roles and whether they experience unique health impacts compared to male firefighters.

Beyond these data gaps, most participants identified barriers to effectively collecting and using data. These findings build upon studies examining data linkage and data registry challenges by identifying department-level data challenges.[51,52] Firefighters and leaders alike acknowledged that asking firefighters to complete data entry is a burdensome task, and leaders noted that this often results in poor quality data. From an institutional standpoint, departments face substantial resource hurdles that impede meaningful data collection or analysis. Departments that still rely on paper forms are unable to conduct basic analysis of trends like the most frequent causes of injury. In some cases, this results in data that is essentially unusable to health and safety personnel who are otherwise equipped to analyze it, and in others, departments also lack the staff to do robust analysis. Without the technology and personnel to effectively track and analyze injuries or fitness statistics, fire departments will be unable to develop prevention activities tailored to their workforces. Even in departments with the software to support data analysis, departments need to be able to hire personnel to examine data in-house or partner with outside researchers.

There may be opportunities to leverage technology to automate data collection and ease administrative burdens. For example, there are resources for individual firefighters to document their exposures through mobile apps.[119] On an organizational level, departments might be able to conduct some automation through their computer aided dispatch systems, which could

provide logs of exposure to structure fires based on call history. With the development of NERIS, the U.S. Fire Administration is already developing a modernized, national data infrastructure that could provide departments with the data structure needed to assess health and safety data. Our findings emphasize the importance of ensuring that NERIS is easy to use, requires low levels of input from firefighters themselves, and relies on automated data inputs as much as possible. The design of new systems like NERIS also offer opportunities to integrate privacy protections into technology, through a "privacy by design" approach. Champions of privacy by design call for building privacy protections directly into data systems.[136] This could include proactive consideration of privacy-oriented designs and minimizing identifiable data access.[136,137] For the fire service, this could mean taking firefighters' preferences for limited sharing of identifiable data into account, and limiting the collection of or access to identifiable information. Fire service stakeholder should incorporate firefighters' data privacy preferences into the very design and structure of new software and other technologies.

Ultimately, many of the challenges participants described stemmed from monetary constraints, which prevented departments from purchasing software or hiring staff to examine health and safety data. Fire departments are publicly funded organizations, and several leaders described serious funding challenges. It will be difficult for many fire departments to justify investments in data if they are struggling to recruit and retain firefighters or purchase new PPE. However, researchers can play a role in helping departments justify the expenses associated with health and safety data collection, and in filling specific data gaps. Research suggests that every firefighter injury results in tens of thousands of dollars in associated costs, and experts have

linked occupational injury prevention writ large to financial savings.[49,138,139] A few participants indicated that they have used data to illustrate the cost savings achieved through injury prevention, which can help justify the funding of health and safety activities. Researchers should partner with departments to assess the potential savings associated with injury reduction programs. Departments may be able to justify investments in injury tracking software or additional health and safety personnel if there is evidence that this can result in overall savings.

Researchers can also play a role in helping departments collect or make sense of existing health and safety data. Firefighters and leaders voiced support for research on health trends within the fire service. While there is a role for ongoing injury surveillance and regular health and fitness measurements within departments, researchers can lend their expertise on discrete projects related to a topic (e.g. mental health, retention of female firefighters) or establishing data infrastructure. Our findings also reiterate the importance of disseminating research findings, both on an individual level and overall study results. Many of the firefighters we spoke with were broadly supportive of research on topics such as cancer but were apathetic about their own contributions. Several described their frustration after sharing sensitive information such as symptoms of psychological distress or biospecimens, and never knowing the purpose or outcome of a study. It is essential that national leaders and researchers communicate clearly about the objectives and findings of their work, particularly as NIOSH rolls out the National Firefighter Registry and fire service researchers conduct ongoing health and safety work. While researchers cannot ensure that findings are translated into practice, they can commit to providing research subjects with individual results that might benefit awareness about their

own health, and to sharing the conclusions of a study. Disseminating research findings is not only ethically responsible but may help bolster trust in data in the fire service, contributing to the much-needed cultural paradigm shift that our participants called for.

Finally, our findings reveal a need for ethical guidance on how to appropriately handle firefighter data. Interestingly, leaders in our sample voiced more concerns about current data practices than firefighters, citing instances in which firefighters resisted data collection or were worried about data access. In general, leaders were more highly attuned to the need for and barriers to ethical data collection, use, and sharing. This might reflect the fact that leadership interact with a wide range of firefighters and are more likely to encounter diverse views than firefighters working in a single fire station. It might also reflect their roles, which grant them responsibilities across a department and require them to consider the ethical and legal obligations surrounding worker data.

While further unpacking these ethical theories is beyond the scope of this study, our findings reflect a need for additional work establishing ethical principles in occupational health and safety settings, including detailed guidance on privacy topics. Although our participants did not raise major alarms about unethical data practices, they described legitimate concerns about ensuring firefighter data privacy, while calling for large amounts of new data collection. Leaders responsible for health and safety would benefit from ethical frameworks and specific guidelines for how to ensure the confidentiality of firefighter data. A few experts have acknowledged the need for confidential data practices, but guidelines for ethical data practices remain general.[44]

The continued refinement of ethical frameworks specific to occupational health and safety professionals, as well as practical guidance on how to implement these frameworks, will help employers implement new data collection efforts in an ethical manner.

Our study is an exploratory examination of data privacy perspectives in the fire service and has several limitations. We encountered recruitment challenges in Maryland that limited the size of our firefighter sample. While we found similar results across Maryland and Virginia, and similarities among firefighters and leadership in Maryland, we may have identified a broader range of opinions in a larger sample. Because this is a qualitative study, our findings are also specific to the geographic jurisdictions and departments that we worked with but are informative for hypothesis generation in the broader context of the fire service. Because fire departments were recruited through study team networks, they had a history of participating in research, and likely differed from other departments across the country. Attitudes towards data privacy may differ based on department culture, trust in leadership, staffing (e.g. hybrid volunteer/career), and geography. Future research should explore this topic in a wider range of departments. Our sample was also largely white and male; while this reflects the overall demographics of the fire service, more research is needed to understand how perspectives on data might vary based on gender and race.[60] Finally, while some participants discussed mental health data, we focused on physical health and safety data. We discovered a desire for more mental health data collection alongside fears about how mental health information could be used in punitive or discriminatory ways. More work is needed to examine perceptions of mental health data amid ongoing efforts to destigmatize mental health and offer services to firefighters.

Conclusion

Our findings reflect enthusiasm about the role of data in protecting firefighter health and safety alongside frustration about the lack of resources and infrastructure for high quality data collection and analysis. Participants identified specific data gaps, funding challenges, technological priorities, and cultural shifts needed to maintain a fit workforce, process firefighter benefits, and enable sophisticated injury prevention programs. These findings can inform ongoing efforts to modernize the fire service's data infrastructure and conduct research on firefighter health and safety.

Table 3.1 Participant roles by jurisdiction

	VA	MD	National	Total
Total	38	16	11	65
Firefighters				
Career FFs	30	1	-	31
Union leaders	1	1	-	2
Leadership				
Department	7	14	-	21
Government	-	-	3	3
Advocacy	-	-	6	6
Research	-	-	2	2

Table 3.2 Participant characteristics by role

	Firefighters	Leadership
Gender		
Male	29	21
Female	4	11
Race		
White	30	24
Non-white	3	8
Age (mean years)	36	48
Experience (mean years)	12	25

Notes: One firefighter did not report age. Two leadership participants did not report years of experience.

Table 3.3 Overview of themes

Themes	Firefighters	Leadership	Summary
Current data practices			
Kinds of data collected	X	X	Departments collected a range of health, injury, fitness, and exposure data. Government officials and researchers collected injury and fatality data.
Data access, sharing, and reporting practices	X	X	All participants described limited sharing of identifiable data and adequate protections for most health and safety data.
Value of data in the fire service			
Establishing fitness for duty	X	X	Departments used medical, fitness information to establish fitness for duty status.
Obtaining benefits	X	X	Firefighters used injury, exposure information to facilitate workers compensation, presumptive benefits.
Conducting health and safety prevention		X	Departments, researchers, and government officials used injury, health, fitness information to understand trends and design prevention.
Supporting administrative priorities		X	Leaders used data to obtain funding, advance DEI priorities, and advocate for policy change.
Challenges			
Resource and logistical challenges	X	X	Firefighters and leaders described individual administrative burdens. Leaders describe tech and resource challenges.
Cultural factors		X	Leaders encountered resistance to change, lack of emphasis on evidence, and skepticism about data integrity.
Data considerations		X	Leaders described concerns about data sharing and ideal conditions for facilitating data collection, such as de-identification and limiting sharing. Firefighters largely did not share these concerns but favored deidentification.

Job repercussion fears		X	Leaders believed firefighters were resistant to sharing information based on fear of termination or job impacts; many linked this to fears about losing identity as a firefighter. For the most part, firefighters did not share these concerns.
Priorities for addressing gaps			
New data collection	X	X	Firefighters and leaders called for more data in specific areas, such a mental health and exposures.
Strengthening data infrastructure		X	Leadership called for improved technology and data linkages.
Improving data communication	X	X	Firefighters and advocates emphasized the need for data interpretation and dissemination. Leaders acknowledged the importance of communication.

Chapter Four (Manuscript Three): "Data's a double edged sword": Firefighter and fire service leadership preferences regarding wearable technologies and associated data privacy considerations

Abstract

Objective: Despite growing interest in using wearable technology to improve firefighter health and safety, there is little evidence on fire service stakeholders' data privacy preferences. We assessed firefighter and leadership preferences regarding the collection, use, and sharing of wearable data.

Methods: We conducted interviews with fire department leaders and union representatives in Maryland and Virginia, and with leaders in national fire service organizations. We conducted interviews and focus groups with career firefighters in both states. Data collection took place from March – November 2023. We audio recorded interviews and focus groups and analyzed transcripts using thematic analysis.

Results: We conducted 4 focus groups and 35 interviews with 65 total participants (31 firefighters, 2 union leaders, 11 national leaders, and 21 department leaders). We identified 9 themes. Leaders were optimistic about using wearable data to help firefighters obtain benefits, improve safety on calls, conduct prevention, and advance administrative priorities. Firefighters viewed wearables in the context of tradeoffs between safety and autonomy, privacy, and job status. Firefighters opposed using wearable data in real time on calls whereas leadership were

supportive. Participants identified barriers to implementation including logistical, data usability, and cultural factors. Firefighters and leaders described conditions for ethical wearable use including data preferences and communication strategies; many emphasized the need for limited use cases, limited sharing of identifiable data, and individual data access.

Conclusions: Data from wearable devices has the potential to protect firefighter health and safety but must be utilized in a way that respects firefighters' autonomy and data preferences.

Introduction

Firefighters experience high rates of occupational injury and fatality. In 2022, there were 65,000 on-duty injuries and 96 fatalities in the line of duty.[1,2] Although fires account for only 4% of the overall calls in the fire service, a disproportionate share of firefighter injury and fatality occurs on firegrounds: in 2022, 33% of firefighter injuries and 35% of firefighter fatalities occurred at firegrounds.[1,2,113] There is growing interest among fire service leaders, government officials, and researchers in deploying wearable technology on calls to reduce firefighter injury and save lives.[3,4,55,56]

Researchers anticipate that devices worn by individual firefighters will be used to collect biometric, exposure, or geographic location data in real time as they respond to incidents. For example, a firefighter responding to a structure fire might wear clothing outfitted with sensors that collect data on his or her heart rate, blood pressure, temperature, respiratory rate, or ergonomics, as well as real time exposure and location data.[3,4,55,56] An incident commander could use this data to ascertain when firefighters are in distress or reaching short term exposure limits and make corresponding staffing decisions on a fire scene.[3] Experts also envision using wearable data for post-event analysis, in which fire department health and safety staff or researchers could examine health and safety trends. Wearable data could be used to inform department health and fitness training programs, reassess exposure limits, or for research.[3,4] Appendix 4.1 shows examples of wearable devices, associated data, and use cases.

The rise of these new technologies prompts questions about firefighter data privacy and the confidentiality of firefighter data.[3,4] Wearable devices are poised to collect potentially sensitive health information, which could be shared with a firefighter's employer, government entities, or researchers. It is possible that some firefighters are concerned about the general privacy of their information—the extent to which such information is known or used.[27] Others might be more concerned with ensuring that their data is treated confidentially, meaning that their data is handled in accordance with specific constraints on who can access it or how it can be used.[27,140,141] In this paper, we focus primarily on the broader concept of data privacy, although our findings have implications for what confidential data practices in the fire service might entail.

There are few studies that empirically examine data privacy perspectives among fire service stakeholders. A few studies examining firefighter acceptance of wearable technology suggested that firefighters have generalized privacy concerns related to wearable devices, in part based on who might have access to the data and the nature of data collected.[142–144] One study examined the impacts of a biometric device used in training settings on workplace environment. Firefighters in southwestern fire departments viewed devices as having negative impacts on their identity and their relative power within their organizations, and resisted the active use of wearables while responding to calls.[59] Research from other occupational settings suggests that workers are hesitant about sharing biometric information with their employers, and that leadership anticipate these concerns but remain optimistic about the benefits of wearables.[10,45]

While these studies raise important concerns about attitudes towards wearable technology itself, we lack evidence on underlying data privacy preferences in the fire service.

From a normative perspective, there are ethical arguments for assessing firefighter privacy preferences and ensuring they are respected as wearables are implemented. Although there has been little normative work specifically on firefighter data privacy, experts examining wearables in occupational settings generally have called for examinations of employee views.[9,41–43] Many experts cite the biomedical ethics principles of beneficence, non-maleficence, respect for autonomy, and justice when describing employers' obligations to minimize safety risks.[44,145,146] Some emphasize the confidentiality of employee health and safety data as a key component of respecting employees' autonomy.[44] It will be difficult for fire departments to respect their employees' autonomy with relation to wearable data without first understanding their views towards such data, prompting a need for research examining firefighter perspectives. Unpacking firefighter perspectives may help ensure that fire departments can implement wearables in a manner that respects individual autonomy.

In addition to the ethical rationale for assessing firefighters' privacy preferences, there are practical reasons for trying to understand and respect their views. Evidence from other fields indicates that a range of workers have historically resisted workplace surveillance, both through formal channels such as union negotiations, and informal channels through which they alter or evade new technologies.[65,71] If firefighters are averse to sharing biometric information or concerned about their employer accessing health data, they may resist the implementation of

wearable devices. Understanding firefighter preferences is not only ethically justified but may contribute to the successful implementation of wearables.

In light of these considerations, our study examines firefighter and fire service leadership perspectives on wearable data. Firefighters and leaders may have distinct preferences about who should have access to potentially sensitive biometric data and how such data should be used. It is essential that we understand firefighter perspectives alongside the views of department and national-level leaders who might wish to utilize wearables and might be responsible for their implementation. In this study, we examined firefighter and fire service leadership preferences regarding wearable technologies and related data privacy considerations. Our findings reveal the conditions under which firefighters and leaders view new technology as ethically acceptable, and where their views align and diverge.

Methods

We used qualitative methods to explore fire service stakeholders' wearable technology preferences. Given the limited evidence on firefighters' views towards data privacy and technology, we wanted to utilize methods that would allow us to explore a range of perspectives and develop theories about perceptions of data and technology in the fire service. We conducted semi-structured focus groups and interviews with firefighters and fire service leaders.

Sample/recruitment

Our sample consisted of three subgroups with differing roles in the fire service: career (or "paid") firefighters, fire department leaders, and national leaders in government, research, and advocacy organizations. We also included department union leaders in the career firefighter category based on their roles as firefighters advocating for their peers within departments. We sampled career firefighters and fire department leaders from within the same fire departments. A member of our study team created a validated safety climate assessment for the fire service (Firefighter Organizational Culture of Safety (FOCUS)) which is now actively used in practice settings.[121] We selected departments that had participated in FOCUS previously or were actively participating at the time of data collection. We recruited four departments in total: two in Maryland and two in Virginia.

To recruit individual participants within fire departments, we collaborated with a point of contact in each department to invite firefighters to participate in focus groups. Firefighters had to be career rank-and-file firefighters to be eligible to participate. We excluded volunteer firefighters because we were interested in examining occupational health and safety data and wanted to recruit full time employees. We were unable to recruit participants for a focus group in one Maryland department and conducted a semi-structured interview instead. In departments that were unionized, we invited union leaders to participate in a semi-structured interview. To recruit leaders in each department, we worked with our departmental points of contact to invite individuals from overall leadership, health and safety, or human resources (HR) to participate in semi-structured interviews. For national leadership, we invited individuals from

government, research, and advocacy to participate in semi-structured interviews. National level participants were selected using purposeful sampling and snowball sampling.

Data collection

We developed interview and focus group guides for each subgroup that explored views towards wearable technologies and related data in the fire service. For all leadership interviews, we asked open-ended questions about wearable technology and participants' preferences regarding how wearable data should be collected, used, and shared. We tailored the interview guides for each subgroup to account for differences in roles. For firefighter focus groups and interviews, we developed scenarios describing three hypothetical examples of wearable technology: a mandatory biometric vest that would be used in real time on a fireground and after the fact for health and safety; a mandatory wearable sensor collecting exposure data on all calls, to be used in real time and after the fact; and a voluntary health and fitness watch, the data from which firefighters could choose to share with the department. These examples were all modeled on examples from the literature and discussions with department leaders.[3,55] Appendices 4.1-4.6 include interview and focus group discussion questions, and an exit survey for collecting focus group participants' demographic information.

We conducted interviews over Zoom and focus groups in person at fire stations. Some focus groups were held while participating firefighters were on-duty but out of service (e.g. firefighters were not available for responding to calls), whereas for others, firefighters remained in service. For in service groups, if some participants received a call, the group was paused until

they returned or continued without them for a period, always ensuring that half the group remained for the discussion to continue. We collected data from March – November 2023. The interviewer/moderator drafted memos following each interview/focus group to record initial themes and relevant notes.[122] All interviews and focus groups were audio recorded then transcribed verbatim. We obtained oral consent from all participants. This research was approved by the Johns Hopkins Bloomberg School of Public Health Institutional Review Board.

Analysis

We used a thematic analysis approach for data analysis.[122] We began to develop a codebook after partially completing data collection. One team member reviewed the memos and interview/discussion guides and drafted an initial codebook, which was subsequently reviewed and refined by a second team member. These two team members conducted two rounds of double coding transcripts, meeting to compare coding, resolve disagreements, and revise the codebook. The team members then independently coded the remaining transcripts, meeting as needed to discuss questions. Coding was conducted in Dedoose. The codebook is included in Appendix 4.7.

For analysis, we organized stakeholders into two categories: firefighters and leadership. The firefighter category consisted of career firefighters and union representatives, and the leadership category captured department and national leaders. The roles in each group were both conceptually similar (e.g. a firefighter and a firefighter who served in leadership in a local union) and we found similar themes within each group. When describing our findings in this

paper, we focus on these two overall groups, and when relevant indicate if a participant held multiple roles (e.g. an advocate who also worked in a fire department).

Results

Sample

We had a total of 65 participants: 31 career firefighters, 2 union leaders, 11 national leaders, and 21 department leaders. Focus groups ranged in size from 5-9 participants. Due to data collection challenges in Maryland, firefighter participants were predominately from Virginia (see Table 4.1 for an overview of participants by role and jurisdiction). Participants were mostly white and male. The leadership sample was more diverse than the firefighter sample, with a higher share of women (34% vs 12%) and non-white participants (25% vs 9%). Firefighters were less experienced and younger than leaders (mean of 12 years of experience vs. 25; mean of 36 years of age compared to 48). Table 4.2 shows participant characteristics. On average, focus groups were 77 minutes, firefighter interviews were 39 minutes, and leadership interviews were 45 minutes.

Themes

We identified 9 themes. We grouped the themes into 3 overarching categories capturing 1) benefits of wearables, 2) tradeoffs accompanying wearables, and 3) implementation considerations. Table 4.3 shows the categories and themes organized by stakeholder group. While firefighters and leaders agreed on some of the benefits of wearables, firefighters expressed concern about loss of autonomy and privacy, and changes in job status due to

wearables. Leadership were more optimistic about the benefits outweighing any drawbacks. Despite these divergent views, leaders and firefighters both identified practical barriers to implementation and described similar conditions for ensuring the ethical use of wearable data.

Benefits of wearables

Participants anticipated a range of positive impacts from the rollout of wearable technology, including facilitating firefighter benefits, protecting safety on calls, prevention, and administrative priorities.

Facilitating benefits

There was nearly unanimous support among all stakeholder groups for collecting exposure data to support future presumptive benefit claims. Maryland and Virginia both have presumptive benefit laws which designate certain cancers and diseases that are presumed to be work-related, and are designed to facilitate coverage for these conditions.[128,129] Firefighters have indicated that filing for coverage under presumptive benefit laws still requires significant documentation of occupational exposures to prove that a condition was work-related (see Aim 2). Firefighters were particularly enthusiastic about the exposure scenario, which would document exposures to toxins on calls. Many indicated that they preferred this example over the other two scenarios because it had clear benefits to them and fewer potential drawbacks. Several characterized exposure data as inherently less personal:

> Participant 8: That’s fine. Because we're all in the same environment. It'd be all the, you know...
> Participant 3: Yeah, same—
> Participant 5: That'd be the one that's going to help us more.

> Many: Mmhmm, yeah.
> Participant 1: Especially in the long run.
> Participant 5: If then we could use—to me, that's one. Don't even like de-identify. Make that known and make that identifiable. So that way if one of us gets cancer down the road, they got all this data to pull from. – Firefighters

In a few instances, leaders and firefighters expressed concern that collecting biometric or exposure information could backfire on firefighters. For instance, firefighters pointed out that even with exposure documentation, workers compensation might deny their claims, arguing that a firefighter's personal protective equipment should have protected them. Leaders noted that presumptive laws often come with specific eligibility criteria, and if exposure records do not meet these criteria, claims could be denied. However, these participants still supported an exposure wearable, as they believed the benefits would outweigh the risks.

Safety on calls

When initially asked about the general use of wearable technology, many leaders suggested using biometric data while responding to fire calls. Leaders in and outside of departments strongly endorsed the use of biometric wearable data in real time when responding to calls, citing the potential to save lives. Several acknowledged that this might entail the collection of sensitive information such as body temperature, heart rate, or blood pressure, but believed this was justified. One department leader explained:

> I am extremely keen to see [biometric] information operationalized at the street level. And there's two main reasons for that. One I want to be able to know when a firefighter is in distress before they are in distress, or that their vital signs clearly reflect that they are in distress, even if they themselves don't perceive they are, so that I can withdraw them from an IDLH [immediately dangerous to life and health] environment and save their life beforehand . . . And second, I

> want to prevent other firefighters from dying trying to recover a deceased member. – Department Leader

Although firefighters acknowledged this lifesaving potential, only a small share supported this use case. Participants in one focus group endorsed using biometric data on calls, highlighting the potentially life saving impacts. In another group, participants preferred limited use of wearable data on calls, such as only using location data, which was perceived as less personal and more likely to help in the event that a firefighter was lost in a structure fire. Ultimately, participants in three of the four groups were opposed to using biometric data on calls, citing tradeoffs described in more detail below.

Prevention

Nearly all leadership participants were broadly supportive of using a range of wearable devices to improve health and safety. Leaders highlighted a range of potential benefits from sleep, diet, exercise, exposure, and biometric data. They described conducting general health or fitness tracking for individual purposes, or using such data to understand risk factors and trends within a department. Participants from all departments and advocacy organizations discussed the value of offering firefighters access to their own data from a wearable, suggesting that this could be used to empower better individual health and fitness decisions. Several expressed their belief that firefighters had a right to this information and that it might encourage better diet, exercise, or medical practices, resulting in a healthier and fitter workforce. Some department leaders were also excited about using wearables in training environments to track temperature or hydration and prevent injuries.

> I think in a training environment, that would probably be the place where we would start with it . . . We see a lot of injuries in recruit school from folks that are just not used to this type of profession. So to be able to monitor that at a closer level, especially during not only our evolutions, but some of our physical fitness training [would be helpful]. – Department Leader

Some firefighters also noted that health or fitness data could inform individual decision making. There were mixed views on the benefits of an optional fitness device like an Apple Watch or FitBit. Approximately half of firefighters indicated they would opt into participating, with most wanting to use the data to inform decisions about their own health.

> Participant 9: I'm a numbers person. I think in the moment it's just, interesting to see. But aggregate data over a year. When I get back from a call, my heart rate is still pounding for the next 30 minutes. What can I do to drop that before we go to bed? You don't have to use it. And then sleep data would be great too.
> Participant 8: The sleep data is huge.
> Participant 4: Like take it to the doctor if there's abnormalities, take it to trainers and say, hey, this is what I want to train for. How I'm adjusting that.
> Participant 3: My resting pulse over the last year went up 15 beats per minute. I've done everything the same. Why is this trending? – Firefighters

While many firefighters did not express strong opinions about their data being used for department-level prevention or prevention-oriented research, most were comfortable sharing deidentified or aggregated biometric and health data for preventive use cases. Several added caveats around how they would like such data to be shared (described in more detail below) but were broadly supportive of using firefighter data to understand and prevent future injuries.

Advancing administrative priorities

A small number of department leaders described using data from wearables as a tool to justify funding requests. For example, some suggested that this data might help illustrate staffing

needs at a fire by showing how firefighters are overtaxed on a fireground. When asked about the potential impact of technology on diversity, equity, and inclusion (DEI) priorities, leadership participants were mixed on whether technology was a helpful, neutral, or harmful tool. Some characterized data as a tool that could be wielded for positive or negative purposes:

> Again, data's a double-edged sword. And I always look at data as like statistics. I mean, you can pretty much make your data say what you want it to say if you just kind of manipulate it and twist it and handpick, especially when you handpick parts of the data set, right . . . the data is the tool and it's kind of up to, we can go either way with it. – Department Leader

Others in government, advocacy, and departments viewed technology as a tool that could be used to advance DEI priorities in the fire service. For instance, participants thought that having more data on female firefighters could help address gender equity issues. Several explained that the standards for recruitment or recurring fitness exams are based on males, and that women are taught techniques designed for male physiology.

> NFPA [National Fire Protection Association] recommends 12 METS [metabolic equivalents] as the standard aerobic capacity. That's what they recommend for you to be able to do as a firefighter. But females and males biologically, there's a difference when it comes to oxygen uptake . . . Some of our fittest females are still not hitting 12. So, I would say in that sense, if they could collect data on females and see what their work capacity is at a fire, then they would be able to have like, hey, females should be able to hit maybe 11 METS and then males 12 METS kind of thing . . . I think that women are at a disadvantage if the standard is just a group of white males they collected data on that are in college. Which is typically where all fitness data is collected from. – Department Leader

Most firefighters did not discuss administrative benefits of wearable data. We did not directly ask firefighters about their views on DEI impacts, and it did not come up during discussions. Some firefighters suggested that wearable data could be used to make a case for hiring additional staff or increasing funding. Several pointed out that concrete evidence (e.g. on sleep

patterns) could show how difficult their jobs are and the negative impacts on their health. There were mixed views on whether such evidence would result in real changes, but several were hopeful that such data could be used positively.

Tradeoffs

Discussion of the benefits of wearable technology was closely accompanied by concerns about the tradeoffs that would accompany such devices. Firefighters discussed fears about the loss of autonomy and privacy and job status. In some cases, firefighters viewed these tradeoffs as significant enough that they did not support the use of wearable technology. Leaders anticipated some of these concerns but did believe they would be widespread.

Loss of autonomy and privacy

Many firefighters discussed wearable data in the context of the overall risk calculus associated with firefighting. Several pointed out that there are inherent tradeoffs between maintaining their health and safety and performing core job functions like fighting fire. Many believed that wearable data would place undue emphasis on the risks of firefighting, undermining firefighters' decisions to accept these risks in order to protect the public. Participants emphasized their commitment to firefighting despite the sacrifices it might require, and expressed concern that wearable data would threaten their ability to carry out their responsibilities.

> Seems like they always try to take all the risk out of our job. Well, our job is inherently risky anyway. Like we knew that getting into it, we all knew there was a percentage we'd get hurt or maybe even die. Hopefully, that wouldn't happen. But, you know, like the more data and stuff they collect on us sometimes, like the less and less they allow us to do our job, or the harder it is to do our job. – Firefighter

Others viewed a biometric wearable worn on calls as a direct threat to their autonomy on a fireground, inhibiting individual decision making on-scene. They believed that each individual should be able to make their own decisions about how to operate on a call, such as knowing when he or she needed to come out of a structure fire or devote more personal time to recovery. Many were concerned that using wearable data to make real time decisions would inhibit their ability to make decisions and ultimately perform their duties:

> Participant 5: I don't want that. Like if you can use it, if it's going to help somebody down the road. Like if it's data collection we're going to use for the future, that's fine. But don't bring it into where the rubber meets the road because that's where we got to do our job. Like I'd hate to think that a battalion chief—you know, we go to a fire entrapment, and we got a victim in there and the battalion chief is like, "Hey, you got to come out, your heart rate is this." Because I'd say no.
> Participant 3: Me too. – Firefighters

Some of these concerns were related to firefighters' autonomy, whereas others were more privacy-oriented. Firefighters in one group described hesitation about others in the department learning personal information:

> Participant 8: I'd be a little uncomfortable if it was like, oh, [Participant 8] got pulled off the fireground because his blood pressure was 200 over 100. I don't care if these guys [in participant's station] know it, but if the nerds at the [other station] know about it, I don't want them to know about it. [laughter] – Firefighter

For the majority of firefighters, the loss of privacy and autonomy that would accompany a biometric wearable device was too great to justify the use of wearables at an incident. Most concluded that they would not support using a wearable on calls because it would interfere with their ability to do their jobs. In some cases, firefighters opposed using biometric devices on calls when it would be used by leaders in the department to make decisions, but supported

individual use of biometric data from a fitness device (e.g. a personal FitBit). This would allow individual firefighters to benefit from the health information while maintaining their autonomy.

Leaders were attuned to firefighter concerns about privacy, and several anticipated pushback towards wearables based on general ideological resistance to monitoring. Some anticipated more firefighter concerns if the information collected was sensitive (e.g. greater opposition to biometric data collection than exposure data collection) or if data was collected over a longer time period (e.g. an entire shift). Some leaders preemptively suggested limiting the duration of data collection or the settings in which wearables would be used in an effort to protect firefighter privacy. However, most leaders were not overly worried about firefighter privacy concerns. Although many acknowledged the validity of fears about data sensitivity, they stated that their department would not use data inappropriately and thought that firefighters' concerns could be assuaged.

Job status

Firefighters' concerns about autonomy and privacy were closely linked to fears about the impact of wearables on job status. Many believed that biometric data, which was likely to uncover underlying health risks, could be used to fire them.

> The more health and safety stuff we do, sometimes it almost gets to the point where they're almost trying to push you out of your job . . . You know, like sometimes I would rather not even know than them to find some little illness that I lose my job over. And I feel like for us as a department, just knowing how we've been, like if they had that data right at hand. God forbid, my heart rate would reach a certain level and they would pull me off the incident or, you know, or would there be repercussions from it? Like that would be my biggest concern with it. – Firefighter

Several firefighters also worried that biometric or fitness data could be used punitively or could force changes that were not technically punitive but would negatively impact their work, such as changes to the shift schedule, station transfers, or delayed promotions.

> Participant 8: If it would be de-identified it would be fine. The issue would be if it wasn't, someone could pick you out. You get punished all of a sudden because...
> Participant 6: You get nervous. You need remedial training if you get nervous.
> Many: Yeah, yeah.
> Participant 5: I can see that. Like held against you promotionally. – Firefighters

Nearly all leadership participants anticipated some pushback against wearable devices from firefighters. Most believed that a share of firefighters would resist devices collecting health or medical information that could be used to take them off the job, resulting in termination, changes in job status, or simply changing the way the job is done. Several participants described firefighting as an identity, and framed fears about losing one's job as fear about losing identity as a firefighter or losing the community that comes with being a firefighter.

> There's concern among both the career and the volunteer service about how would that data be used? Could I lose my job? In other words, if I had a physiological condition that was identified, could I be taken off the line, where would I work? . . . Firefighting is a passion. A lot of firefighters have a passion for that. And they don't want to give it up. – National Leader

However, most leaders concluded that fears about job repercussions could be overcome. Department leaders stated that they would not use wearable data for punitive or discriminatory purposes and anticipated that a small share of firefighters would oppose wearables. Advocacy participants were more aligned with firefighters, as several expressed

hesitation about sharing identifiable firefighter information with department leadership based on concerns about firefighters losing their jobs.

Implementation considerations

Participants discussed several barriers to implementation, citing concerns about logistics, the usability and quality of wearable data, and cultural factors. Both leadership and firefighters articulated specific preferences regarding how new technology should be deployed, including preferences for data collection, use, and sharing, and messaging and engagement strategies.

Barriers to implementation

Firefighters identified a host of logistical challenges to implementing wearables. In many cases, participants' initial reaction to the wearable scenarios was skepticism about the ease of use or durability. Most wanted to make sure that a wearable would be comfortable and would not delay their response times. Several were frustrated by the amount of protective gear that they were already required to wear and were exhausted by the thought of adding an additional item.

Ultimately, some firefighters suggested that wearable data would be impossible to use on a fireground. Many firefighters were skeptical about the objectivity of data and did not think it was reasonable to use quantitative thresholds to make decisions on calls, as each individual might have his or her own baseline. Most anticipated that everyone on a fire scene would have elevated biometric metrics, and it would be unrealistic to pull a firefighter from a structure fire based on a high heart rate or blood pressure.

> Participant 4: No the idea of like, hey, listen, we want to collect all this to know more about what you're doing and how it's impacting you. That's a great idea. But it would be difficult for me because then they would develop a threshold like, okay, your heart rate can't be over 210. If it's over 210, then it's unsafe. But is it 210 because he's working hard or is it 210 because he's nervous? . . .
> Participant 1: But like everybody's different. Like we're talking about the parameters of like when to pull someone out would have to be...
> Participant 2: Very broad. It would have to be because a lot of times we rely on that adrenaline in the fire, it gives us that boost of strength, whatever, that we need. So, the parameters would just have to be very...
> Participant 1: Extremely high, extremely low. – Firefighters

Others pointed out that even if the data was available on a fire scene, an incident commander is already inundated with information, and tactical objectives should take priority. Some anticipated that if an incident commander had access to biometric data and a firefighter experienced an adverse event like a cardiac event on scene, it would place greater liability on the department for adverse events.

Several firefighters indicated that it was also unrealistic to use biometric or health data outside of calls, such as for prevention. Some described a history of the fire service or departments failing to act on evidence, suggesting that there was no point to collecting more data if it would not be used. Others expressed the belief that there is sufficient evidence on many health risks. One firefighter questioned the benefit of collecting biometric data to inform health and fitness programs:

> I guess what I'm saying is, the changes they're going to want to make from that data you can make without even having the data. Like we know that we need to be in shape. We know that we need to be working out. We know that we need to be getting ready to do our job. So you don't really need the data to push those initiatives because it's a known fact. – Firefighter

Leadership participants described a range of barriers to successfully implementing wearables, largely related to resource limitations and device design and maintenance. Leaders across stakeholder group anticipated resource challenges, as wearables would be costly for individual departments, and likely too expensive for small, rural, or volunteer departments. Many department leaders were skeptical that their departments could obtain funding or persuade local governments to adopt a subscription model. Leaders shared firefighters' concerns that devices would not be able to stand up to fire conditions and noted the challenges of maintaining existing equipment or getting firefighters to wear bulky devices.

Some leadership participants believed that fire department culture and fire service culture as a whole would hinder the implementation of wearables. Many leaders cited a general resistance to change, especially from older generations of firefighters who liked things they way they had always been done. They anticipated that acceptance of new technology would split on generational lines. One national leader and former firefighter stated:

> Since you're diving into the role of the fire service, there are two phrases that you should know. Number one, the fire service is 200 years of tradition unimpeded by progress. Two, the two things the fire service hates the most are change for one and two, the way things have always been. To answer your question, this is where generationally, there's going to be a huge dichotomy. – National Leader

A few firefighters acknowledged a general resistance to change but did not raise this as a serious barrier to implementation. Some discussed concerns about negative impacts of wearables on department culture that might lead to resistance towards new devices. For instance, in one group, firefighters anticipated negative cultural impacts if a wearable collected

sleep data that led to station transfers. Some indicated that firefighters would resist these kinds of changes on the basis that they would be poor for morale, ultimately hindering implementation.

Preferences for data collection, use, and sharing

Firefighters called for preventing, or at least limiting, the sharing of identifiable data, although they had mixed views on who such data should be shared with. Firefighters in one group preferred to keep identifiable information within their departments and share only deidentified information with external entities like researchers:

> Like if we're doing something for the greater good, that's not a deep dive on me and doesn't identify me personally, then I'd be all for that. – Firefighter

In other groups, firefighters were more comfortable with sharing their data externally, and did not want their information accessible to leadership within the department:

> I would [be] fine being monitored, but I wouldn't want our department to have it. If it's going out for research or whatever, I'm completely okay with that. – Firefighter

Firefighters also emphasized the importance of having access to their own data for the prevention and benefits use cases described earlier. Several noted that they had a right to access their own data in a timely and easily accessible fashion to use as they wished. A few also expressed a preference for using wearable data during training as opposed to during calls.

Leaders across stakeholder groups were aligned with firefighters in supporting individual data access and limiting the spread of identifiable information. Some department leaders noted that

they would sometimes want to use identifiable wearable data, such as if it was being used to track vital signs on a fireground. However, most indicated that they would limit access to identifiable information on a need-to-know basis, sharing it only with an incident commander at a fire scene or with health and safety personnel. Many supported deidentifying data for research and only sharing aggregated trends within their departments.

Leaders also suggested implementing wearables in limited settings and limiting use cases. Some favored using wearable data for research purposes as opposed to ongoing departmental priorities. Other leaders indicated that they would limit data collection to work settings or only during certain work tasks. Several department leaders suggested using wearables only in training or recruitment settings, where they could be deployed in a controlled environment and preempt concerns about ongoing surveillance:

> Especially if we're using full gear and air packs to run through scenarios or whatever, days when we're training where, we don't have the 120-degree days here, but we have 98 degrees and 98 percent humidity days. So, anytime we were worried about heat stress or something like that for a particular training evolution, I think it could be a really good benefit for that. – Department Leader

Leaders also emphasized the importance of ensuring that wearable data was used in nonpunitive ways that would benefit firefighters, and storing data securely. Most department leaders and advocates suggested making wearables voluntary, at least at the outset, to gain buy in.

Messaging and engagement strategies

Department leaders and advocates emphasized the need for communication and stakeholder engagement to effectively implement wearables. A department leader described the need to share wearable data with firefighters in a digestible format:

> I think we could do a better job of communicating out to the field. I think data would come into [the] health and safety bureau. And then from there they take that aggregate data and they push it out to the field in some format that people can actually look at it and understand it and appreciate it . . . I just think data is no good if you don't share it with people, right? Like, if people don't know what they don't know, and I think that's part of what our issue is, is we're not sharing enough information. – Department Leader

Other leaders described the need to gain buy in from trusted leaders like the local union, or to build trust with individual firefighters. Some department and advocacy leaders also supported partnering with the international union or national figures such as leaders from major metropolitan fire departments. Participants also emphasized the importance of highlighting the benefits to firefighters, explaining the use case for firefighter data, and clearly communicating who would have access to firefighter data. A few department and advocacy leaders suggested drawing parallels to existing technology, such as self-contained breathing apparatus (SCBA), to assuage firefighter fears that new devices would disrupt their work.

> I think there would be definitely more acceptance if the firefighters knew we were doing it for their protection. It's just like when self-contained breathing apparatus were introduced to the fire service, there was resistance from the old timers, and then now it's the standard. You wear it from the time you get on scene until the overhaul is done . . . So, I think the same thing would be used for the biometric data. Hey, we're using this to protect you, if you get too hot or if the temperature that you're in is too hot, we're going to pull you out and make recommendations. I think it would be adopted pretty well. – Department Leader

Firefighters were less focused on communication, but emphasized that they wanted to understand the purpose behind collecting wearable data, and would need to see positive

impacts to support long term use. One firefighter noted that she expected the union to engage if the department planned to implement a wearable.

Discussion

Our findings capture enthusiasm about the promise of wearable technology alongside serious hesitations about the use and sharing of wearable data. In line with research in other occupational settings, we uncovered that leadership viewed wearables as a powerful tool for saving lives, but that this was coupled with firefighter concerns about their autonomy and livelihoods.[10] This dichotomy was most apparent for the use of biometric data in real time on calls. Consistent with a prior study examining a biometric device in the fire service, we found that firefighters were concerned about their autonomy on a fire scene.[59] However, our participants situated their concerns in the context of the broader relationship between health and safety and autonomy. Firefighters identified a core tension between doing their jobs, which come with inherent hazards, and mitigating health and safety risks. The tradeoffs that accompany wearables lie on a spectrum, in which some participants were willing to take on greater risks to preserve their autonomy, and others preferred to emphasize risk mitigation.

Experts have highlighted the importance of respect for worker autonomy in the context of an employer's ethical obligations to provide a safe workplace, including respect for the confidentiality of health and safety data.[44,145,146] While data confidentiality is an important priority which we discuss in more detail below, our findings suggest that respecting firefighter autonomy requires an expansive understanding of autonomy as a concept. The firefighters in

our sample emphasized that they had each decided to enter a high-risk occupation and wanted to be afforded the ability to make their own decisions about acceptable risk on a day-to-day basis. Most preferred to maintain their autonomy rather than use a wearable on calls, even if the wearable was designed to protect them.

These findings offer insights on the impact of technology and data on the relationship between worker autonomy and worker safety. There are limited studies examining the confluence of occupational health and safety, autonomy and risk, and data. The occupational health and safety literature suggests that worker autonomy is positively associated with attitudes towards health and safety behaviors.[147,148] Researchers examining job autonomy and safety climate in the mining industry found that an autonomous workplace was linked with perceptions of safety climate and compliance.[147] A survey of police officers discovered that autonomous motivation, in which behavior change is self-motivated, was correlated with self-reported adherence to safety protocols and commitment to injury prevention.[148] However, from a data privacy perspective, workplace surveillance negatively impacts worker autonomy.[26,65] Research on the trucking industry indicates that drivers resist workplace surveillance, in part based on autonomy, and that efforts to monitor this worker population have met fierce resistance.[65] Our findings suggest that there is inherent tension in health and safety technology, in which monitoring workers can improve their safety but infringes on their autonomy. Future efforts to deploy health and safety technology in the fire service should attempt to balance these tradeoffs. Our findings on firefighters' preferred conditions for using wearables, detailed below, offer insights into how this might be carried out.

Our work builds upon the existing literature on wearables in the fire service by identifying specific preferences for how different kinds of wearable data should be used. Participants were more comfortable with wearables that collected exposure data than those collecting health or fitness information. Participants in leadership as well as rank-and-file firefighters overwhelmingly endorsed using wearable technology to collect exposure data. Researchers, technology developers, and fire departments should prioritize the development and use of devices that can document exposures. As firefighters pointed out, this data could help them obtain presumptive benefits, and so the design of an exposure wearable should account for the kinds of data that firefighters need to file for benefits. Beyond individual-level benefits, exposure data could be used to expand our understanding of the occupational hazards that firefighters encounter and evaluate exposure limits.

Participants also shed light on the conditions under which wearable data could be ethically utilized, describing the need for limiting the settings in which wearables were deployed and developing restrictions on how wearable data could be used or shared. In line with previous studies in the fire service and other occupational settings, participants suggested that departments should try deploying biometric devices in limited settings such as in training or during recruitment or fire academy activities.[45,59,149] Collecting biometric data in training environments might prevent injury and fatality without threatening firefighters' autonomy on a fire scene or ability to provide services. In general, leadership participants favored making any wearable program voluntary, at least initially, to gain trust and buy in from their staff. This aligns

with research in other sectors which indicates that both employers and employees prefer voluntary wearable programs.[45,149] Offering wearables as voluntary measures might help build confidence in the benefits of technology while respecting individual firefighters' privacy preferences.

From a data standpoint, many participants emphasized the need to deidentify firefighter data, prevent punitive use of data, and share findings with individual firefighters. Even though firefighters did not reach consensus on who they thought should have access to their information, there was strong support for deidentifying and aggregating firefighter data if it was going to be used by health and safety staff or researchers. While there is very little research on empirical data preferences in occupational health and safety settings, these findings align with prescriptive suggestions found in the normative literature on data privacy in occupational settings.[41–44,71,150] In future instances where firefighter data might be reported to government agencies or researchers, such data should be stripped of identifiers. More work should also be done to determine the feasibility of truly deidentifying or anonymizing firefighter data.

Our findings also reflect a need to ensure that the collection and use of firefighter data is accompanied by safeguards to prevent retaliation or discrimination. Firefighters raised concerns about explicitly punitive actions, such as termination, as well as less overtly negative consequences such as station transfers. These concerns echo those surrounding workplace wellness programs, in which employees fear that their decisions to disclose health information (or not) will be penalized.[71,151,152] Departments or researchers utilizing wearables should ensure

that they are accompanied by policies that clearly define how data will be used (e.g. only for health and safety purposes) or prohibit punitive use cases. These kinds of protections could serve as a starting point for what confidential treatment of firefighter data might look like. In unionized departments, the union can play a role in negotiating for these protections. Union contracts in Maryland and Virginia contain a range of provisions related to data privacy; some do not address data privacy considerations at all whereas others authorize general surveillance for health and safety purposes (see Aim 1). Going forward, unions may wish to negotiate specific limits on when wearables could be used and prohibitions on using data punitively or sharing identifiable data.

Firefighters also indicated that if they are asked to share personal information, they should receive access to their individual level data along with interpretation of the results both on an individual and population level. Sharing the findings from a wearable program or study will not only help ensure the ethical rollout of a device, but may also bolster trust in wearables generally, and their potential for improving health and safety outcomes. There is extensive research ethics literature that offers insights on best practices for returning individual research results to participants, such as using plain language, contextualizing findings, and allowing for questions.[153,154] While health and safety practitioners may not be required to uphold specific ethical standards that researchers must adhere to regarding informed consent or return of results, these best practices illustrate how anyone collecting firefighter data should consider sharing findings with participants.

Collectively, participants' preferred conditions for the collection, use, and sharing of wearable data offer insights on the parameters that might constitute confidential treatment of firefighter health and safety data. The confidentiality of health or medical information is typically discussed in the context of a provider-patient relationship or in a research context, in which a patient or a research subject expects that his or her information will only be used or shared in authorized ways.[141] There is some professional guidance for occupational health and safety professionals requiring that they maintain the general confidentiality of employee information, but few specifics on what confidentiality means in occupational contexts.[155–157] In addition, not all employer representatives who might access firefighter data are health or safety professionals, and most are not medical professionals, and may not be bound by these professional codes of conduct. While some of our participants' preferences address larger questions related to data privacy (e.g. whether wearables data should be used on a fire call), others reveal what confidential use of data might entail (e.g. providing researchers access to deidentified data to use for injury prevention). Future research should further unpack the factors that constitute confidentiality in an occupational context.

Finally, in addition to these normative preferences, participants highlighted a number of structural or logistical challenges to implementing wearables. Departments or jurisdictions will need to consider how to fund new technology, which might require new funding models for subscription services, negotiations with technology companies over data storage and ownership, and obtaining funds. Participants across stakeholder groups also raised concerns about the wearability and durability of wearable devices in the context of the fireground and

the demanding environments in which they work. While not the primary focus of this study, these logistical challenges may pose major hurdles to implementing new technology in the fire service, and merit additional consideration.

Our study has limitations. We spoke with a smaller number of firefighters in Maryland compared to Virginia due to data collection challenges. We attempted many different strategies for recruiting Maryland firefighters and attribute low recruitment rates to a variety of factors including an overworked and understaffed workforce, survey fatigue, and scheduling challenges. While we did not find differences across states, speaking with more Maryland firefighters may have revealed a wider range of opinions. Our sample was largely white and male, in line with the overall demographics of the fire service. Women in our sample identified opportunities for data to help advance gender equity, although evidence from other occupational settings suggests that women are less likely to support workplace surveillance than men.[39,45] We did not discover differences based on race, but a large body of work has established the ways in which technology is often not designed for or accessible to racial minorities, and how data is often used in discriminatory fashion.[158,159] While we did gain some insights on the perspectives of underrepresented minorities in the fire service, future research should focus on unpacking the preferences of women and racial minorities. Our study also focused on career firefighters, although volunteer firefighters might be asked to use wearable technology and their views might vary based on their positions as volunteers. Future research should examine this topic among a wider range of fire departments to assess views across geographic location and department culture. The examples of wearable technology that participants discussed were

theoretical, and the focus group scenarios varied in terms of the type of technology and voluntariness. Our findings captured participants' expressed views but might differ from actual preferences in a practice setting. Future research should systematically unpack the factors associated with willingness to participate in a wearable intervention, such as the type of device, kind of data collected, or data access provisions.

Conclusion

Firefighters and fire service leaders are optimistic about using wearable technology to document firefighter exposures, but expressed diverging views on the acceptability of using biometric data in real time on calls. Participants characterized their preferences in terms of the tradeoffs accompanying wearable data, which could be used to save lives and bolster health and safety, but also threatens firefighter autonomy, privacy, and job status. Despite this disagreement, firefighters and leaders discussed specific conditions under which they would support wearables, including using biometric data in limited settings or in voluntary programs, limiting access to identifiable data, prohibiting punitive use of wearable data, and ensuring high quality communication about firefighters' data.

Table 4.1 Participant roles by jurisdiction

	VA	MD	National	Total
Total	38	16	11	65
Firefighters				
Career FFs	30	1	-	31
Union leaders	1	1	-	2
Leadership				
Department	7	14	-	21
Government	-	-	3	3
Advocacy	-	-	6	6
Research	-	-	2	2

Table 4.2 Participant characteristics by role

	Firefighters	Leadership
Gender		
Male	29	21
Female	4	11
Race		
White	30	24
Non-white	3	8
Age (mean years)	36	48
Experience (mean years)	12	25

Notes: One firefighter did not report age. Two leadership participants did not report years of experience.

Table 4.3 Overview of themes by stakeholder group

Themes	Firefighters	Leadership	Summary
Benefits			
Facilitating benefits	X	X	Firefighters and leadership were optimistic about using wearable exposure data to facilitate benefits
Safety on calls		X	Firefighters saw limited use for biometric wearables on calls, whereas fire leadership strongly endorsed using biometric data to save lives on a fireground
Prevention	X	X	Leadership saw potential for using biometric and health/fitness data to enhance injury prevention efforts. Firefighters sought individual-level prevention.
Advancing administrative priorities		X	Some leaders described potential for wearable data to help obtain funding and to advance diversity, equity, and inclusion in the fire service.
Tradeoffs			
Loss of autonomy, privacy	X		Firefighters expressed serious concerns about the tradeoffs accompanying biometric and health/fitness devices. Leaders had mild concerns about privacy.
Job status	X	X	Firefighters were concerned that biometric and health/ fitness wearables could result in job loss, punitive action, or changes in job status if they uncovered health risks. Leaders anticipated this but thought this concern could be overcome or was overblown.
Implementation considerations			
Barriers to implementation	X	X	Firefighters and leaders raised logistical concerns. Firefighters were skeptical about data subjectivity and some leaders thought resistance to change would impede implementation.

Preferences for data collection, use, and sharing	X	X	Firefighters called for limiting, or ideally preventing, sharing of identifiable data in departments. Firefighters and leaders wanted to ensure access to individual data. Leaders suggested implementing biometric and health/fitness data in limited settings and use cases.
Messaging and engagement strategies	X	X	Leadership, especially in advocacy organizations, and firefighters emphasized the need for education, trusted messengers, union engagement, and conveying the benefits to firefighters.

Chapter Five: Conclusion

This dissertation examined data privacy in the fire service, assessing the regulatory environment, current data practices, and preferences for future data collection. Collectively, the three aims reveal the strengths and limitations of the fire service's existing data efforts, and offer insights on future research, policy, and practice. This chapter summarizes the findings of each aim, discusses overall study strengths and limitations, and lays out the implications for researchers, policymakers, and practitioners.

Summary of findings

Aim 1 examined the public policies governing career firefighter occupational health and safety data in Maryland and Virginia. There were few laws and regulations specifically addressing occupational health and safety data privacy considerations, reflecting a need for additional policymaking to ensure the privacy of firefighter data. Union contracts contained the most granular provisions and illustrated potential paths forward in future policymaking. As fire departments consider collecting additional health and safety data, unions may be best equipped to negotiate for safeguards specific to their members' preferences.

Aim 2 assessed firefighter and leadership perceptions of current data practices. While participants viewed data as a tool for protecting firefighters, they expressed frustration with gaps in existing data and resource limitations that hindered sophisticated data analysis. Our findings revealed a need for greater collection of exposure and mental health data, investments

in data infrastructure, and high quality communication about the purpose of data collection and dissemination of results among firefighters.

Aim 3 explored firefighter and leadership preferences regarding wearable devices and the data generated by new technology. We found conflicting views between firefighters and leadership with regards to using biometric data for safety purposes on calls. Firefighters framed their views towards wearables in terms of tradeoffs between health or safety and autonomy, privacy, and job status. Despite these complexities, firefighters and leaders identified conditions for the appropriate use of wearables and called for specific limits on data collection, use, and sharing.

Limitations and strengths

This dissertation has limitations that are important to consider while interpreting the findings and that can inform future research. Aim 1 served as an initial exploration of policies governing firefighter occupational health and safety data, but did not include guidance or case law. Including a broader range of documents might shed light on the full range of policies that dictate how firefighter data is collected, used, stored, and accessed. For Aims 2-3, although the goal of qualitative research is not to produce generalizable findings, our findings may have limited transferability to other jurisdictions or populations. This dissertation was limited to Maryland and Virginia, and the findings are specific to career or hybrid fire departments in our sample. Firefighters across the country operate in diverse settings, reflecting a range of geography, population density, hazards, and call volume. Departments also vary significantly in terms of their organizational policies, cultures, and staffing (e.g. fully career, hybrid

volunteer/career). We did not include volunteer firefighters, who often undergo similar fitness for duty evaluations or injury reporting as career firefighters. Nor did we include fire departments in other geographic regions, where hazards may vary based on climate and environmental threats (e.g. wildland fires in the western United States). Our findings also reflect participants' expressed views towards data privacy and technology. Firefighter and leadership attitudes might differ when faced with an actual data initiative or wearable device, or when provided with detailed implementation plans instead of hypothetical scenarios.

Despite these limitations, this dissertation has several strengths that bolster its contributions to the literature and to policy and practice. It is the first to comprehensively examine firefighter data privacy using empirical methods. Our findings contribute novel insights on firefighter and leadership preferences regarding current and future data practices. The study design allowed for in depth comparisons of firefighter and leadership perspectives, providing a holistic assessment of data privacy preferences among fire service stakeholders. These findings, along with the results from Aim 1, reveal a comprehensive view of current data practices in the fire service and opportunities for future policymaking and research. The findings from Aim 3, which reveal specific and practical parameters for how wearables should be implemented, can be applied in practice settings to inform the ethical deployment of wearables. And while our findings may not be directly transferable to other occupational settings, they offer ideas as to how workers in similar fields like law enforcement or the military might view health and safety data collection and wearables.

Research implications

This dissertation contributes to the nascent literature on occupational health and safety data privacy. It revealed the need for additional research to address data gaps that participants identified, new research priorities for understanding data privacy preferences in the fire service, and principles for how researchers should disseminate their findings.

Filling data gaps in the fire service

Participants in Aims 2-3 identified data gaps that researchers can help fill. Some participants called for additional data collection or analysis within departments. For instance, several leaders described the need for more detailed injury data collection and mental health information. Other participants wanted to see more research on trends across the fire service, such as on occupational cancers and exposures to toxic substances. And a small number highlighted the importance of research on underrepresented minorities in the fire service. For instance, participants called for studying recruitment and retention of women and racial minorities and for updating health and fitness standards based on female physiology. Researchers possess the expertise necessary to tackle these kinds of research questions, which might require national-level data collection and injury epidemiology methods. In some cases, researchers have already begun to study these topics.[132,134,160] As external entities, researchers might also be better equipped to collect sensitive data from firefighters who do not wish to share personal information with leaders in their departments. While not all the firefighters in our sample were resistant to internal data sharing, participants discussed the sensitivity of mental health information and noted that firefighters are reluctant to disclose mental health information with

peers or leaders. Collecting data on confidential topics such as mental health might face less resistance if it is carried out by outside researchers.

Future research on occupational health and safety data privacy

This dissertation established an initial assessment of data privacy in the fire service and illuminates areas for future research on this topic. Within the fire service, future research should attempt to quantify firefighter and leadership perspectives on data privacy to produce generalizable findings on their views. Researchers could assess the share of stakeholders who support policy reforms or conditions for using wearables. There are also opportunities to expand this research to other occupational populations, including workers in similar, high-risk fields like law enforcement officials and military service members. Future research should explore whether our findings hold in other settings, especially in fields with high injury rates but less hierarchical cultures such as construction or mining.

Studies can continue to assess theoretical preferences as well as worker feedback regarding the actual implementation of a new data collection program or wearable device. For example, our participants emphasized the importance of providing firefighters with their own data and interpreting this information. However, research on return of results in a research context suggests that this can be a challenging process, requiring careful consideration of what to do with incidental results and translating information into easily understood formats.[154,161] Researchers could evaluate the acceptability of various models for fire departments to use

when sharing health or medical information with firefighters and the effectiveness of these models in communicating findings to workers.

Disseminating research findings

Participants in Aims 2-3 discussed the need for a cultural paradigm shift towards data. Researchers can contribute to this cultural shift by ensuring that fire service research informs participants about the purpose of a study and communicates the findings to individual firefighters. Firefighters were frustrated by instances in which they shared personal information but were not adequately informed about the purpose of data collection or never received results. Without clear and concise communication about research aims or findings, firefighters may lose faith in the value of research or grow apathetic about the power of evidence to help keep them safety and healthy.

Policy implications

This dissertation offers insights on the strengths and limitations of existing public policies governing firefighter health and safety data in Maryland and Virginia. The findings across all three aims highlight opportunities for public policymaking and union negotiations to secure firefighter data privacy protections, authorize funding, and strengthen presumptive benefit laws.

Future public policymaking

Our findings can inform future public policymaking that aims to ensure firefighter occupational health and safety data is handled in a way that is respectful of firefighters' preferences. There is robust debate among data privacy scholars about the best path forward for public policymaking on data privacy.[27,71,162] Data in occupational settings could be governed by general privacy policies, employment-specific policies, or sector-specific policies. Data privacy protections could also be integrated into technology itself, in a "privacy by design" approach.[136,163] While recommending a mechanism for future policy development is beyond the scope of this dissertation, our findings identify privacy goals that should be incorporated into future policies. Aim 1 identified several gaps in current policies, including a limited number of policies specifically addressing occupational health and safety data or the fire service, and few policies that explicitly limited access to or sharing of employee data. While participants in Aim 2 were largely comfortable with how departments collect, use, and share firefighter data, they called for greater data collection and in Aim 3 expressed preferences for how such data should be handled. Future policymaking should limit access to sensitive health and safety information and prohibit using this data in discriminatory or punitive fashion. These kinds of reforms will be all the more important as new technologies, including but not limited to wearables, become commonplace in the coming years.

Future opportunities for union engagement

This dissertation also emphasizes the importance of unions in shaping policies governing occupational health and safety data. The union contracts we reviewed in Aim 1 varied significantly, but several contained granular provisions related to health and safety data. In

some cases, contracts imposed limits on access to medical or injury information, and several contracts required that firefighters be given access to their own data, including exposure documentation. These protections align well with firefighter preferences that we discovered in Aims 2 and 3, and serve as an example of the kinds of data-related provisions that other unions may wish to secure. Alternatively, the two contracts we identified in Virginia authorized general electronic monitoring for health and safety purposes without detailing storage or sharing guidelines. While one contract prohibited proactively using such data for punitive purposes, neither contract comprehensively addressed data privacy concerns. None of the contracts we identified specifically addressed the collection, use, storage, or sharing of wearable data. Aim 3 identified serious concerns among firefighters about wearable data, and suggested that fire department leaders and the rank and file have differing views towards this data. Unions should consider if and how to include provisions protecting wearable data in future contracts, beginning with the conditions identified in Aim 3.

Policies to support department-level data collection

While there are important national-level efforts to update the fire service's incident reporting infrastructure, department leaders consistently emphasized the need for funding to support department-level data collection and analysis.[54] Leaders in all of the fire departments in our sample believed that collecting and analyzing health and safety trends could help improve the wellbeing of their workforces. If departments had basic software to track injuries or health and safety personnel devoted to conducting this analysis, they could design interventions tailored to the needs of their firefighters. Policymakers at the national level could authorize assistance

through grant programs, such as the Assistance to Firefighters Grant Program, which funds priorities including the implementation of wellness and fitness priorities.[164] On the local level, policymakers could allocate funds to strengthen their jurisdictions' data capabilities. Although this will require additional funding, evidence suggests that prevention results in financial savings long term, and these investments might ultimately pay dividends.[49,138,139]

Aligning presumptive benefit laws with data availability

While there are many state-level presumptive benefit laws, including in Maryland and Virginia, participants indicated that firefighters struggle to obtain the documentation needed to obtain such benefits.[128,129] Policymakers designing these laws in other states or updating existing laws should consider the limited exposure documentation that many firefighters have access to. If presumptive laws are truly designed to provide coverage for firefighters, they should not require large amounts of exposure data that most firefighters will be unable to produce.

Practice implications

Finally, this dissertation offers insights on how fire departments, technology developers, and other fire service stakeholders can contribute to the ethical handling of firefighter data. Aim 2 indicated that fire departments currently collect a range of health and fitness information from their workforces, and Aims 2 and 3 suggested that leaders are eager to collect more firefighter data. The Aim 3 findings, which laid out firefighter and leadership preferences regarding the use of wearable data, outline priorities for future data collection and best practices for protecting firefighter privacy.

Ethical collection, use, and sharing of department-level data collection

As departments consider using new technologies, including wearables that will significantly increase data collection, they should limit the use and sharing of data in accordance with firefighter preferences. For example, if departments plan to implement a wearable, they should consider making it optional, engaging with the union or other firefighter representatives, and communicating clearly about the purpose of the device. They should also commit to restricting the use of such data only to health and safety purposes, limiting access to identifiable data, and providing firefighters with their own data. These kinds of stipulations were raised by both firefighters and leadership, suggesting that these safeguards might be favored throughout departments. While we found less consensus on using wearables in real time on calls, piloting devices in limited settings such as training environments and implementing these privacy protections, may build trust in wearables and data long term. These recommendations also align well with suggested guidelines from the normative literature on occupational health and safety ethics.[41]

Technological priorities

Departments and technology companies can also prioritize collecting data that is highly valued by firefighters and leaders. There was strong consensus on the need for additional exposure documentation. Departments should consider strategies for documenting fire exposures through their computer aided dispatch (CAD) systems, and look into software tools for automatically recordings these events, through systems such as NFORS.[119] Technology

companies developing devices for the fire service should prioritize the development of software systems or wearable devices that will automate exposure data collection and provide firefighters with easy access to a log of their career exposures.

Summary

Firefighters take on extraordinary personal risks to keep their communities healthy and safe. Each year thousands of firefighters sustain injuries in the course of their duties and dozens are killed in the line of duty.[1,2] There is essential work being done in fire departments, government agencies, advocacy organizations, and research institutions to protect firefighter health and safety. Much of these efforts entail the collection of personal health, medical, or fitness information. While these initiatives hold great power to safeguard firefighters, they will only be effective if firefighters are willing to share personal data and feel comfortable with how their information will be used and shared. This dissertation assessed the current state of affairs for firefighter data privacy and opportunities for strengthening current public policies and department-level practices. The findings establish a baseline understanding of firefighter preferences and priorities for ensuring that future data collection is conducted in an ethical manner.

References

1. Campbell R, Jay T. Petrillo. Fatal Firefighter Injuries in the US in 2022. Published online June 2023:18.

2. Campbell, Richard, Hall, Shelby. *United States Firefighter Injuries in 2022*. National Fire Protection Association; 2023:16. https://www.nfpa.org/education-and-research/research/nfpa-research/fire-statistical-reports/firefighter-injuries-in-the-united-states

3. Grant, Casey, Hamins, Anthony, Bryner NP, Jones AW, Koepke GH. *Research Roadmap for Smart Fire Fighting*. National Institute of Standards and Technology; 2015:NIST SP 1191. doi:10.6028/NIST.SP.1191

4. Amidon TR, Williams EA, Lipsey T, Callahan R, Nuckols G, Rice S. Sensors and gizmos and data, oh my: informating firefighters' personal protective equipment. *Commun Des Q*. 2018;5(4):15-30. doi:10.1145/3188387.3188389

5. Employer-Reported Workplace Injuries and Illnesses, 2021-2022 - 2022 A01 Results. Published November 8, 2023. Accessed January 22, 2024. https://www.bls.gov/news.release/osh.nr0.htm

6. Fatal work injuries up in 2022 : The Economics Daily: U.S. Bureau of Labor Statistics. Accessed January 22, 2024. https://www.bls.gov/opub/ted/2023/fatal-work-injuries-up-in-2022.htm

7. Brown J. Nearly 50 years of occupational safety and health data : Beyond the Numbers: U.S. Bureau of Labor Statistics. Published July 2020. Accessed November 1, 2021. https://www.bls.gov/opub/btn/volume-9/nearly-50-years-of-occupational-safety-and-health-data.htm

8. National Safety Council. Work Injury Costs. Injury Facts. Accessed November 1, 2021. https://injuryfacts.nsc.org/work/costs/work-injury-costs/

9. Kritzler M, Bäckman M, Tenfält A, Michahelles F. Wearable technology as a solution for workplace safety. In: *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia*. MUM '15. Association for Computing Machinery; 2015:213-217. doi:10.1145/2836041.2836062

10. Schall MC, Sesek RF, Cavuoto LA. Barriers to the Adoption of Wearable Sensors in the Workplace: A Survey of Occupational Safety and Health Professionals. *Hum Factors*. 2018;60(3):351-362. doi:10.1177/0018720817753907

11. Harris A, Sims R, Roberts A. BioErgo Surveillance: New Approaches for Total Worker Health. Synergist Blog. Published November 19, 2020. https://www.aiha.org/blog/bioergo-surveillance-new-approaches-for-total-worker-health

12. Weed J. Wearable Tech That Tells Drowsy Truckers It's Time to Pull Over. *The New York Times*. https://www.nytimes.com/2020/02/06/business/drowsy-driving-truckers.html. Published February 6, 2020. Accessed August 8, 2022.

13. PepsiCo to boost wearable technology use after Frito-Lay workers see injury reductions. Supply Chain Dive. Accessed January 19, 2022. https://www.supplychaindive.com/news/pepsico-frito-lay-kinetic-reflex-wearable-technology/608329/

14. Howard J, Murashov V, Cauda E, Snawder J. Advanced sensor technologies and the future of work. *Am J Ind Med*. 2022;65(1):3-11. doi:10.1002/ajim.23300

15. Wearable Help. The Synergist. Accessed January 21, 2022. https://synergist.aiha.org/201605-wearable-help

16. *Recommended Practices for Safety and Health Programs*. Occupational Safety and Health Administration; 2016:40. https://www.osha.gov/sites/default/files/OSHA3885.pdf

17. Voluntary Protection Programs | Occupational Safety and Health Administration. Accessed January 18, 2022. https://www.osha.gov/vpp

18. OSH Act of 1970 | Occupational Safety and Health Administration. Accessed March 21, 2022. https://www.osha.gov/laws-regs/oshact/section5-duties

19. Electronic Communications Privacy Act of 1986 (ECPA). Bureau of Justice Assistance. Accessed December 6, 2021. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

20. How much employee monitoring is too much? Accessed December 6, 2021. https://www.americanbar.org/news/abanews/publications/youraba/2018/january-2018/how-much-employee-monitoring-is-too-much-/

21. 29 CFR § 1630.14 - Medical examinations and inquiries specifically permitted. LII / Legal Information Institute. Accessed December 6, 2021. https://www.law.cornell.edu/cfr/text/29/1630.14

22. GDPR compliance checklist for US companies. GDPR.eu. Published March 22, 2019. Accessed December 6, 2021. https://gdpr.eu/compliance-checklist-us-companies/

23. State Laws Related to Digital Privacy. Accessed December 6, 2021. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

24. Food and Drug Administration. General Wellness: Policy for Low Risk Devices - Guidance for Industry and Food and Drug Administration Staff. Published online September 27, 2019:12.

25. Covered Entities and Business Associates. HHS.gov. Published November 23, 2015. Accessed December 5, 2021. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

26. Ajunwa I, Crawford K, Schultz J. Limitless Worker Surveillance. California Law Review. Published 2017. Accessed March 25, 2022. https://www.californialawreview.org/print/3-limitless-worker-surveillance/

27. Richards N. *Why Privacy Matters*. Oxford University Press; 2021.

28. Kerry CF, Morris Jr. JB, Chin CT, Turner Lee NE. Bridging the Gaps: A path forward to federal privacy legislation. Published online June 2020:84.

29. Christofides E, O'Doherty K. Company disclosure and consumer perceptions of the privacy implications of direct-to-consumer genetic testing. *New Genet Soc*. 2016;35(2):101-123. doi:10.1080/14636778.2016.1162092

30. Marreiros H, Tonin M, Vlassopoulos M, Schraefel MC. "Now that you mention it": A survey experiment on information, inattention and online privacy. *J Econ Behav Organ*. 2017;140:1-17. doi:10.1016/j.jebo.2017.03.024

31. Vail MW, Earp JB, Antón AI. An Empirical Study of Consumer Perceptions and Comprehension of Web Site Privacy Policies. *IEEE Trans Eng Manag*. 2008;55(3):442-454. doi:10.1109/TEM.2008.922634

32. Adjerid I, Peer E, Acquisti A. *Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making*. Social Science Research Network; 2018. doi:10.2139/ssrn.2765097

33. Auxier B, Rainie L, Anderson, Monica, Perrin, Andrew, Kumar M, Turner E. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center: Internet, Science & Tech. Published November 15, 2019. Accessed January 20, 2022. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

34. Norberg PA, Horne DR, Horne DA. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *J Consum Aff*. 2007;41(1):100-126. doi:10.1111/j.1745-6606.2006.00070.x

35. Ball K. Workplace surveillance: an overview. *Labor Hist*. 2010;51(1):87-106. doi:10.1080/00236561003654776

36. Holland PJ, Cooper B, Hecker R. Electronic monitoring and surveillance in the workplace: The effects on trust in management, and the moderating role of occupational type. *Pers Rev*. 2015;44(1):161-175. doi:10.1108/PR-11-2013-0211

37. Ball K, Daniel EM, Stride C. Dimensions of employee privacy: an empirical study. *Inf Technol People*. 2012;25(4):376-394. doi:10.1108/09593841211278785

38. Chory RM, Vela LE, Avtgis TA. Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. *Empl Responsib Rights J*. 2016;28(1):23-43. doi:10.1007/s10672-015-9267-4

39. Stark L, Stanhaus A, Anthony DL. "I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance. *J Assoc Inf Sci Technol*. 2020;71(9):1074-1088. doi:10.1002/asi.24342

40. Oz E, Glass R, Behling R. Electronic workplace monitoring: What employees think. *Omega*. 1999;27(2):167-177. doi:10.1016/S0305-0483(98)00037-1

41. Svertoka E, Saafi S, Rusu-Casandra A, et al. Wearables for Industrial Work Safety: A Survey. *Sensors*. 2021;21(11):3844. doi:10.3390/s21113844

42. Maltseva K. Wearables in the workplace: The brave new world of employee engagement. *Bus Horiz*. 2020;63(4):493-505. doi:10.1016/j.bushor.2020.03.007

43. Mettler T, Wulf J. Physiolytics at the workplace: Affordances and constraints of wearables use from an employee's perspective. *Inf Syst J*. 2019;29(1):245-273. doi:10.1111/isj.12205

44. Rogers B, Schill AL. Ethics and Total Worker Health®: Constructs for Ethical Decision-Making and Competencies for Professional Practice. *Int J Environ Res Public Health*. 2021;18(19):10030. doi:10.3390/ijerph181910030

45. Jacobs JV, Hettinger LJ, Huang YH, et al. Employee acceptance of wearable technology in the workplace. *Appl Ergon*. 2019;78:148-156. doi:10.1016/j.apergo.2019.03.003

46. Laroche E, L'Espérance S. Cancer Incidence and Mortality among Firefighters: An Overview of Epidemiologic Systematic Reviews. *Int J Environ Res Public Health*. 2021;18(5):2519. doi:10.3390/ijerph18052519

47. Lee DJ, Ahn S, McClure LA, et al. Cancer risk and mortality among firefighters: a meta-analytic review. *Front Oncol*. 2023;13:1130754. doi:10.3389/fonc.2023.1130754

48. Demers PA, DeMarini DM, Fent KW, et al. Carcinogenicity of occupational exposure as a firefighter. *Lancet Oncol*. 2022;23(8):985-986. doi:10.1016/S1470-2045(22)00390-4

49. Butry DT, Webb D, Gilbert S, Taylor J. *The Economics of Firefighter Injuries in the United States: Executive Summary*. Fire Protection Research Foundation; 2019. Accessed July 25, 2022. https://www.nfpa.org/-/media/Files/News-and-Research/Fire-statistics-and-reports/Emergency-responders/RFFFCostOfInjuryExecutiveSummary.ashx

50. McClure LA, Koru-Sengul T, Hernandez MN, et al. Availability and accuracy of occupation in cancer registry data among Florida firefighters. *PloS One*. 2019;14(4):e0215867. doi:10.1371/journal.pone.0215867

51. Kahn SA, Mosier M. Firefighter Injury Data Are Wrought With Discrepancy: Pearls From the National Burn Repository. *J Burn Care Res Off Publ Am Burn Assoc*. 2018;39(4):623-625. doi:10.1093/jbcr/irx025

52. Widman SA, LeVasseur MT, Tabb LP, Taylor JA. The benefits of data linkage for firefighter injury surveillance. *Inj Prev J Int Soc Child Adolesc Inj Prev*. 2018;24(1):19-28. doi:10.1136/injuryprev-2016-042213

53. National Firefighter Registry | NIOSH | CDC. Published April 25, 2022. Accessed July 22, 2022. https://www.cdc.gov/niosh/firefighters/registry.html

54. About the National Emergency Response Information System (NERIS). U.S. Fire Administration. Published May 9, 2023. Accessed July 23, 2023. https://www.usfa.fema.gov/nfirs/neris/about-neris/

55. Weidinger J. What is known and what remains unexplored: A review of the firefighter information technologies literature. *Int J Disaster Risk Reduct*. 2022;78:103115. doi:10.1016/j.ijdrr.2022.103115

56. Taborri J, Pasinetti S, Cardinali L, Perroni F, Rossi S. Preventing and Monitoring Work-Related Diseases in Firefighters: A Literature Review on Sensor-Based Systems and Future Perspectives in Robotic Devices. *Int J Environ Res Public Health*. 2021;18(18):9723. doi:10.3390/ijerph18189723

57. ActiveAlert. Active911. Accessed July 26, 2022. https://active911.com/activealert/

58. Carpenter D, McLeod A, Hicks C, Maasberg M. Privacy and biometrics: An empirical examination of employee concerns. *Inf Syst Front*. 2018;20(1):91-110. doi:10.1007/s10796-016-9667-5

59. Rumsey A, Le Dantec CA. Clearing the Smoke: The Changing Identities and Work in Firefighters. In: *Proceedings of the 2019 on Designing Interactive Systems Conference*. ACM; 2019:581-592. doi:10.1145/3322276.3322292

60. Employed persons by detailed occupation, sex, race, and Hispanic or Latino ethnicity : U.S. Bureau of Labor Statistics. Accessed January 3, 2024. https://www.bls.gov/cps/cpsaat11.htm

61. Sorensen G, Dennerlein JT, Peters SE, Sabbath EL, Kelly EL, Wagner GR. The future of research on work, safety, health and wellbeing: A guiding conceptual framework. *Soc Sci Med*. 2021;269:113593. doi:10.1016/j.socscimed.2020.113593

62. Li Y. Theories in online information privacy research: A critical review and an integrated framework. *Decis Support Syst*. 2012;54(1):471-481. doi:10.1016/j.dss.2012.06.010

63. Campbell R. United States Firefighter Injuries in 2021.

64. NIOSH Launches the National Firefighter Registry for Cancer to Understand and Reduce Cancer in the Fire Service. CDC. Published January 1, 2016. Accessed July 27, 2023. https://www.cdc.gov/media/releases/2023/p0417-firefighter-cance-registry.html

65. Karen Levy. *Data Driven: Truckers, Technology, and The New Workplace Surveillance*. Princeton University Press; 2022.

66. Joshua Valentino. Setting the framework for biometric privacy legislation after the "big bang" of biometrics in the workplace. *Hofstra Labor Employ Law J*. 2020;38(1):37.

67. Andrew Schuman. Who's Checking? A proposal to protect employee health screening data. *Hofstra Labor Employ Law J*. 2021;39(1):37.

68. Anne G. Bibeau. *Employee Privacy Laws: Virginia*. Westlaw; 2022:18.

69. Fiona W. Ong, Elizabeth Torphy-Donzella, Shawe Rosenthal. *Employee Privacy Laws: Maryland*. Westlaw; 2022:22.

70. Search the National Fire Department Registry. Accessed July 26, 2023. https://apps.usfa.fema.gov/registry/search

71. Ifeoma Ajunwa. *The Quantified Worker: Law and Technology in the Modern Workplace*. Cambridge University Press; 2023.

72. Presumptive Health Initiative. IAFF. Accessed July 23, 2023. https://www.iaff.org/presumptive-health/

73. 29 CFR § 1913.10.

74. Md. Code Ann. Comm. Law § 14-3504.

75. Va. Code Ann. § 2.2-203.2:4.

76. Memorandum of Understanding Fiscal Years 2022-2024 between the Mayor and City Council of Baltimore and Baltimore Fire Fighters Local 734, IAFF AFL-CIO, CLC.

77. Memorandum of Understanding Between the Baltimore County Administration and the Baltimore County Professional Fire Fighters Association IAFF Local 1311.

78. Agreement Between Montgomery County Career Fire Fighters Association, International Association of Fire Fighters, Local 1664, AFL-CIO and Montgomery County

Government/Montgomery County, Maryland For the Years July 1, 2022 Through June 30, 2024.

79. Agreement Made By and Between Prince George's County, Maryland and International Association of Fire Fighters Local No. 1619 (Fire Fighters, Paramedics and Fire Fighter/Medics) July 1, 2022 Through June 30, 2024.

80. Collective Bargaining Agreement Between Arlington Professional Firefighters and Paramedics Assoc., IAFF Local 2800, and Arlington County Government July 1, 2023 Through June 30, 2026.

81. Collective Bargaining Agreement Between the City of Alexandria, Virginia and the International Association of Fire Fighters Local 2141 Effective From July 1, 2023- Jun 30, 2026.

82. 15 U.S.C. § 2201 et seq.

83. 29 U.S.C. § 651 et seq.

84. 29 CFR § 1602.

85. 29 CFR § 1910.1020.

86. 29 CFR § 1904.

87. 42 U.S.C. § 12101 et seq.

88. 42 U.S.C. § 2000ff et seq.

89. 42 U.S.C. § 2601.

90. State Plans | Occupational Safety and Health Administration. Accessed July 26, 2023. https://www.osha.gov/stateplans/

91. Md. Code Ann. Lab. & Empl. 3-701.

92. Va. Code Ann. § 65.2-900(A).

93. Va. Code Ann. § 40.1-51.1(D).

94. Va. Code Ann. § 65.2–402.

95. 16VAC25-60-80.

96. Va. Code Ann. §8.01-413.1.

97. Va. Code Ann. § 59.1–593 through 59.1-602.

98. Memorandum of Agreement, Anne Arundel County and Local 1563 IAFF.

99. Collective Bargaining Agreement Between the Town of Ocean City, Maryland and Career Fire Fighter Paramedics Association of Ocean City, IAFF Local 4269, International Association of Firefighters, Local 4269, AFL-CIO Effective July 1, 2019 - June 30, 2022 (later amended through 2024).

100. Agreement Between the City of Hagerstown, Maryland and International Association of Fire Fighters, Local Number 1605 Effective July 1, 2018 - June 30, 2022.

101. *IAFF Local 1715 Collective Bargaining Agreement with the Mayor and City Council of Cumberland, MD July 1, 2017 through June 30, 2020*.

102. Memorandum of Understanding between the State of Maryland and the Baltimore/Washington International Airport Professional Fire Fighters Local 1742 IAFF, AFL-CIO, CLC January 1, 2022-December 31, 2024.

103. 1913.10 - Rules of agency practice and procedure concerning OSHA access to employee medical records. | Occupational Safety and Health Administration. Published 2020. Accessed December 6, 2021. https://www.osha.gov/laws-regs/regulations/standardnumber/1913/1913.10

104. 45 CFR § 160 and 164.

105. Improve Tracking of Workplace Injuries and Illnesses. Federal Register. Published March 30, 2022. Accessed May 31, 2023. https://www.federalregister.gov/documents/2022/03/30/2022-06546/improve-tracking-of-workplace-injuries-and-illnesses

106. Va. Code Ann. § 40.1-58.

107. Elizabeth R. Guzman. *HB582 Employees of Local Governments; Collective Bargaining*.; 2020. Accessed July 26, 2023. https://lis.virginia.gov/cgi-bin/legp604.exe?201+sum+HB582

108. Kristin. VA Local Ratifies State's First Contract in 40 years. IAFF. Published February 10, 2023. Accessed July 26, 2023. https://www.iaff.org/news/va-local-ratifies-states-first-contract-in-40-years/

109. Rizzo S. Arlington signs first contract with fire and EMS union since 1975. *Washington Post*. https://www.washingtonpost.com/dc-md-va/2023/06/27/arlington-fire-ems-collective-bargaining-agreement/. Published June 27, 2023. Accessed July 26, 2023.

110. *Union Members - 2022*. Bureau of Labor Statistics; 2023:13. Accessed July 23, 2023. https://www.bls.gov/news.release/pdf/union2.pdf

111. Studnicka A. The Emergence of Wearable Technology and the Legal Implications for Athletes, Teams, Leagues and Other Sports Organizations across Amateur and Professional Athletics. *DePaul J Sports Law*. 2020;16(1):[i]-224.

112. Rita Fahy, Ben Evarts, Gary P. Stein. *U.S. Fire Department Profile | NFPA Research*. National Fire Protection Association; 2022. Accessed December 1, 2023. https://www.nfpa.org/education-and-research/research/nfpa-research/fire-statistical-reports/us-fire-department-profile

113. Fire Department Overall Run Profile as Reported to the National Fire Incident Reporting System (2020). 2020;22(1).

114. Jahnke SA, Poston WSC, Jitnarin N, Haddock CK. Health Concerns of the U.S. Fire Service: Perspectives from the Firehouse. *Am J Health Promot*. 2012;27(2):111-118. doi:10.4278/ajhp.110311-QUAL-109

115. Kenneth W. Fent, Miriam Siegel, Alexander Mayer, Andrea Wilkinson. *National Firefighter Registry Protocol*. NIOSH; 2023:82. Accessed January 31, 2024. https://www.cdc.gov/niosh/bsc/nfrs/pdfs/NFR-Protocol-approved-5-3-2023_508.pdf

116. About NFIRS. U.S. Fire Administration. Accessed January 16, 2024. https://www.usfa.fema.gov/nfirs/about/

117. NFIRS 5.0 Self-Study Program: Fire Service Casualty Module: NFIRS-5.

118. David Alexander, Lori Moore-Merrell, Steve Kerber, Adam K. Thiel. On Demand Access to Modernizing the U.S. Fire Data System: An Introduction to the National Emergency Response Information System. Webinar presented at: 2023. https://fsri.org/program-update/demand-access-modernizing-us-fire-data-system-introduction-national-emergency

119. NFORS | International Public Safety Data Institute. Accessed January 16, 2024. https://i-psdi.org/nfors-overview.html

120. Moore-Merrell L. The Importance of Data to the Fire Service. Firehouse. Published May 17, 2021. Accessed January 16, 2024. https://www.firehouse.com/tech-comm/article/21219731/the-importance-of-data-to-the-fire-service

121. Taylor JA, Davis AL, Shepler LJ, et al. Development and validation of the fire service safety climate scale. *Saf Sci*. 2019;118:126-144. doi:10.1016/j.ssci.2019.05.007

122. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol*. 2006;3(2):77-101. doi:10.1191/1478088706qp063oa

123. Dedoose Version 9.0.17. Published online 2021. www.dedoose.com

124. NFPA 1582 Standard Development. Accessed January 4, 2024. https://www.nfpa.org/codes-and-standards/1/5/8/nfpa-1582

125. Stanley IH, Hom MA, Hagan CR, Joiner TE. Career prevalence and correlates of suicidal thoughts and behaviors among firefighters. *J Affect Disord*. 2015;187:163-171. doi:10.1016/j.jad.2015.08.007

126. U.S. Fire Administration hosts 2023 Summit on Fire Prevention and Control. U.S. Fire Administration. Accessed January 29, 2024. https://www.usfa.fema.gov//about/usfa-events/2023-10-10-usfa-summit/

127. Vargas de Barros V, Martins LF, Saitz R, Bastos RR, Ronzani TM. Mental health conditions, individual and job characteristics and sleep disturbances among firefighters. *J Health Psychol*. 2013;18(3):350-358. doi:10.1177/1359105312443402

128. Presumptive Disability Law in Virginia. IAFF. Accessed January 24, 2024. https://www.iaff.org/presumptive-health/va/

129. Presumptive Disability Law in Maryland. IAFF. Accessed January 24, 2024. https://www.iaff.org/presumptive-health/md/

130. Jahnke SA, Gist R, Poston WSC, Haddock CK. Behavioral Health Interventions in the Fire Service: Stories from the Firehouse. *J Workplace Behav Health*. 2014;29(2):113-126. doi:10.1080/15555240.2014.898568

131. Harvey SB, Milligan-Saville JS, Paterson HM, et al. The mental health of fire-fighters: An examination of the impact of repeated trauma exposure. *Aust N Z J Psychiatry*. 2016;50(7):649-658. doi:10.1177/0004867415615217

132. Jahnke SA, Poston WC, Haddock CK, Jitnarin N, Hyder ML, Horvath C. The health of women in the US fire service. *BMC Womens Health*. 2012;12(1):39. doi:10.1186/1472-6874-12-39

133. Yoder JD, Aniakudo P. When pranks become harassment: The case of african American women firefighters. *Sex Roles*. 1996;35(5):253-270. doi:10.1007/BF01664768

134. Jung AM, Jahnke SA, Dennis LK, et al. Occupational factors and miscarriages in the US fire service: a cross-sectional analysis of women firefighters. *Environ Health*. 2021;20(1):116. doi:10.1186/s12940-021-00800-4

135. Jahnke SA, Haddock CK, Jitnarin N, Kaipust CM, Hollerbach BS, Poston WSC. The Prevalence and Health Impacts of Frequent Work Discrimination and Harassment among Women Firefighters in the US Fire Service. *BioMed Res Int*. 2019;2019:e6740207. doi:10.1155/2019/6740207

136. Cavoukian A. Privacy by Design: the 7 Foundational Principles. Published online 2006.

137. Schaar P. Privacy by Design. *Identity Inf Soc*. 2010;3(2):267-274. doi:10.1007/s12394-010-0055-x

138. Bushnell PT, Pana-Cryan R, Howard J, Quay B, Ray TK. Measuring the benefits of occupational safety and health research with economic metrics: Insights from the National Institute for Occupational Safety and Health. *Am J Ind Med*. Published online March 15, 2022. doi:10.1002/ajim.23347

139. Business Case for Safety and Health - Benefits | Occupational Safety and Health Administration. Accessed January 26, 2024. https://www.osha.gov/businesscase/benefits

140. Joly Y, Knoppers BM. *Routledge Handbook of Medical Law and Ethics*. Routledge; 2014.

141. Allen A. Privacy and Medicine. In: Zalta EN, ed. *The Stanford Encyclopedia of Philosophy*. Spring 2021. Metaphysics Research Lab, Stanford University; 2021. Accessed February 7, 2024. https://plato.stanford.edu/archives/spr2021/entries/privacy-medicine/

142. Tucker S, Jonnalagadda S, Beseler C, Yoder A, Fruhling A. Exploring wearable technology use and importance of health monitoring in the hazardous occupations of first responders and professional drivers. *J Occup Health*. Published online November 9, 2023:uiad002. doi:10.1093/joccuh/uiad002

143. Carpenter D, Maasberg M, Hicks C, Chen X. A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system. *Int J Inf Manag*. 2016;36(5):735-747. doi:10.1016/j.ijinfomgt.2016.02.013

144. Weidinger J, Schlauderer S, Overhage S. Is the Frontier Shifting into the Right Direction? A Qualitative Analysis of Acceptance Factors for Novel Firefighter Information Technologies. *Inf Syst Front*. 2018;20(4):669-692. doi:10.1007/s10796-017-9785-8

145. Iavicoli S, Valenti A, Gagliardi D, Rantanen J. Ethics and Occupational Health in the Contemporary World of Work. *Int J Environ Res Public Health*. 2018;15(8):1713. doi:10.3390/ijerph15081713

146. Lindhout P, Reniers G. Involving Moral and Ethical Principles in Safety Management Systems. *Int J Environ Res Public Health*. 2021;18(16):8511. doi:10.3390/ijerph18168511

147. Haas E, Ryan M, Hoebbel C. Job Autonomy & Safety Climate: Examining Associations in the Mining Industry. *Prof Saf*. 2018;63(12):30-34.

148. Chan DKC, Webb D, Ryan RM, et al. Preventing occupational injury among police officers: does motivation matter? *Occup Med*. 2017;67(6):435-441. doi:10.1093/occmed/kqx076

149. le Feber M, Jadoenathmisier T, Goede H, Kuijpers E, Pronk A. Ethics and Privacy Considerations Before Deploying Sensor Technologies for Exposure Assessment in the

Workplace: Results of a Structured Discussion Amongst Dutch Stakeholders. *Ann Work Expo Health*. 2021;65(1):3-10. doi:10.1093/annweh/wxaa093

150. Ajunwa I, Crawford K, Ford JS. Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs. *J Law Med Ethics J Am Soc Law Med Ethics*. 2016;44(3):474-480. doi:10.1177/1073110516667943

151. Hendricks-Sturrup RM, Cerminara KL, Lu CY. A Qualitative Study to Develop a Privacy and Nondiscrimination Best Practice Framework for Personalized Wellness Programs. *J Pers Med*. 2020;10(4):264. doi:10.3390/jpm10040264

152. Chung CF, Gorm N, Shklovski IA, Munson S. Finding the Right Fit: Understanding Health Tracking in Workplace Wellness Programs. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM; 2017:4875-4886. doi:10.1145/3025453.3025510

153. Hintz EA, Dean M. Best Practices for Returning Research Findings to Participants: Methodological and Ethical Considerations for Communication Researchers. *Commun Methods Meas*. 2020;14(1):38-54. doi:10.1080/19312458.2019.1650165

154. Downey AS, Busta ER, Mancher M, Botkin JR. Principles for the Return of Individual Research Results: Ethical and Societal Considerations. In: *Returning Individual Research Results to Participants: Guidance for a New Research Paradigm*. National Academies Press (US); 2018. Accessed January 23, 2024. https://www.ncbi.nlm.nih.gov/books/NBK525079/

155. International Labor Organization. International Code of Ethics for Occupational Health Professionals. Accessed January 26, 2024. https://www.iloencyclopaedia.org/part-iii-48230/ethical-issues/item/337-international-code-of-ethics-for-occupational-health-professionals

156. Standards of Occupational and Environmental Health Nursing. *Workplace Health Saf*. 2012;60(3):97-103. doi:10.1177/216507991206000301

157. American College of Occupational and Environmental Medicine. Code of Ethics. ACOEM. Published 2022. Accessed January 26, 2024. https://acoem.org/about-ACOEM/Governance/Code-of-Ethics

158. Allen AL. Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform. Published online February 20, 2022. doi:10.2139/ssrn.4022653

159. Ruha Benjamin. *Race After Technology: Abolitionist Tools for the New Jim Code*. Polity Press; 2019.

160. Horn GP, Fent KW, Kerber S, Smith DL. Hierarchy of contamination control in the fire service: Review of exposure control options to reduce cancer risk. *J Occup Environ Hyg*. 2022;19(9):538-557. doi:10.1080/15459624.2022.2100406

161. Miller FG, Mello MM, Joffe S. Incidental findings in human subjects research: what do investigators owe research participants? *J Law Med Ethics J Am Soc Law Med Ethics*. 2008;36(2):271-279, 211. doi:10.1111/j.1748-720X.2008.00269.x

162. Nissenbaum H. A Contextual Approach to Privacy Online. *Daedalus*. 2011;140(4):32-48. doi:10.1162/DAED_a_00113

163. Privacy by Design. General Data Protection Regulation (GDPR). Accessed January 25, 2024. https://gdpr-info.eu/issues/privacy-by-design/

164. Assistance to Firefighters Grants | FEMA.gov. Published September 20, 2023. Accessed January 24, 2024. https://www.fema.gov/grants/preparedness/firefighters/assistance-grants

Appendices

Appendix 2.1 Search terms

We conducted separate Westlaw searches for federal laws, federal regulations, Maryland laws, Maryland regulations, Virginia laws, and Virginia regulations using each of the following search strings:

((data /s privacy) /p (workplace occupation! employ! worker! employee!))
((data /s health safety) /p (workplace occupation! employ! worker! employee!))
((monitor* surveill*) /s (workplace occupation! employ! worker! employee!))
fire /s data
fire /s health safety

Appendix 2.2 Summary of data privacy provisions

1. Americans with Disabilities Act (ADA), 42 U.S.C. § 12101 et seq.

Jurisdiction
Federal law

1.1 Covered entities
State and local government employers, regardless of size (Title II)

1.2 Covered data
Disability information; medical examinations aimed at disability.

1.3 Data collection permissions
Restrictive: employers cannot ask applications about disability or require medical examinations. Employers may ask about candidates' ability to perform job-related tasks and may require a standardized medical exam for all new hires, and voluntary medical exams as part of a health program.

1.4 Data use
Anti-discrimination: employers cannot use medical or disability information to discriminate in any employment activities (including hiring, firing, pay, promotion, benefits).

1.5 Data storage
Location: medical information (including results from medical exams) must be stored in medical files separate from personnel files).

1.6 Data access
Limited access and sharing: medical files or information about disability must be treated as confidential. This information may only be shared with select people, including supervisors if they need the information to make reasonable accommodations; first aid and safety personnel in the event of emergencies; ADA enforcement officials; and workers compensation offices.

1.7 Additional notes
Title I relates to equal employment opportunities for private employers and state and local governments with 15 or more employees. Title II covers all state and local government employers and their activities.

2. Genetic Information Nondiscrimination Act (GINA), 42 U.S.C. § 2000ff et seq.

Jurisdiction
Federal law

2.1 Covered entities
All employers with 15 or more employees (including state and local government); employment agencies, labor organizations, federal government employees (excluding military).

2.2 Covered data
Genetic information obtained from employee genetic tests, family members' genetic tests, family medical history, or request for and receipt of services by an employee or family member; information about an employee or family member's fetus.

2.3 Data collection permissions
Restrictive: employers cannot request, require, or purchase genetic information about applicants or employees. Select exceptions include: voluntary wellness programs, voluntary genetic monitoring (or as required by law), publicly available sources, FMLA compliance, DNA testing for law enforcement purposes.

2.4 Data use
Anti-discrimination: employers cannot use genetic information to discriminate in any employment activities (including hiring, firing, pay, and promotion).

2.5 Data storage
Location: genetic information must be kept stored in medical files separate from personnel files.

2.6 Data access
Limited access and sharing: genetic information must be treated as confidential. Sharing and access are allowed in select instances, including with: occupational or health researchers conducting research; upon written request from employee or family member; in response to a court order; with federal enforcement officers; for FMLA compliance; or with a public health agency in an emergency (e.g. infectious disease outbreak).

2.7 Additional notes
N/A

3. Family and Medical Leave Act (FMLA), 42 U.S.C. § 2601

Jurisdiction
Federal law

3.1 Covered entities
Public employers of any size (including federal, state, and local employers); employers with 50 or more employees in 20 or more workweeks in the previous year.

3.2 Covered data
FMLA medical information; FMLA dates, communications, and documents on benefits and leave; payroll and employee identification data.

3.3 Data collection permissions
Permissive: employers may request medical information to certify an employee's eligibility for FMLA leave and fitness for duty certification upon return to work; employers may also ask a medical provider to confirm fitness for duty certification. Employees are responsible for associated costs.

3.4 Data use
Benefits: medical information may be used to certify FMLA leave or fitness for duty upon return; records are intended to be used for related recordkeeping.

3.5 Data storage
Location: employers must retain FMLA medical information in a confidential medical file that is separate from the employee's personnel file.
Duration: employers must retain FMLA medical information and communication for at least three years.

3.6 Data access
Limited access and sharing: FMLA medical information must be treated as confidential in compliance with the ADA and GINA; information may only be shared with supervisors as needed to inform work restrictions/accommodations, first aid and safety personnel, and government officials conducting enforcement.

3.7 Additional notes
N/A

4. Federal Fire Prevention and Control Act of 1974, 15 U.S.C. § 2201 et seq.

Jurisdiction
Federal law

4.1 Covered entities
Public and private career and volunteer firefighters.

4.2 Covered data
Voluntary disclosures of injury and fatality information, including causes and nature of injury, and associated property losses.

4.3 Data collection permissions
Mandated: mandated the creation of the National Fire Data Center to collect information on firefighter fatalities and injuries. Reporting of injury data is voluntary. The Data Center must collect information on injuries requiring medical treatment by a doctor (stratified by type of firefighter), deaths that occur while preparing for work or a test, injuries and deaths from motor vehicle accidents and aircraft crashes. The Data Center may develop standardized data reporting methods, encourage and assist agencies in participating, and use existing public and private resources. Electronic reporting must be available.

4.4 Data use
Injury surveillance: data should be used to understand national trends, identify problem areas, set priorities accordingly, identify solutions, and monitor programs designed to reduce fire losses.

4.5 Data storage
Location: the National Fire Incident Reporting System (NFIRS) must be accessible online and updated in real time.

4.6 Data access
Encouraged aggregate sharing: must disseminate information to the greatest extent possible while protecting firefighter medical information in accordance with HIPAA and other relevant federal regulations.

4.7 Additional notes
While reporting is voluntary, FEMA encourages participation by requiring that recipients of Assistance to Firefighters Grants report during their award period. NFIRS is being replaced by the National Emergency Response Information System, designed to be a modernized, interoperable analytic platform.

5. Occupational Safety and Health Act of 1970, 29 U.S.C. § 651 et seq.

Jurisdiction
Federal law

5.1 Covered entities
Private employers engaged in business affecting commerce (state employees in MD and VA are covered based on state OSHA plans).

5.2 Covered data
Records of work-related fatalities, injuries, and illnesses (other than minor injuries not resulting in treatment, loss of consciousness, or changes to work); employee exposure records (to potentially toxic materials or harmful physical agents).

5.3 Data collection permissions
Mandated: authorizes the Secretary of Labor to issue regulation requiring that employers must maintain and update accurate records of employee fatalities, injuries, illnesses, and exposures.

5.4 Data use
Injury surveillance: comparing exposures relative to federal standards (and taking corrective action if needed); making reports.

5.5 Data storage
Duration: records must be maintained for two years.

5.6 Data access
Required employee access: employers must make copies of exposure records available to employees.

5.7 Additional notes
Applies to MD, VA firefighters due to state OSHA plans.

6. 29 CFR § 1602 Recordkeeping Regulation

Jurisdiction
Federal regulation

6.1 Covered entities
State and local governments, private employers, and their employees; labor organizations.

6.2 Covered data
Personnel and employment records including hiring, accommodation requests, promotion, layoff, termination, pay, tenure, and other terms.

6.3 Data collection permissions
N/A

6.4 Data use
N/A

6.5 Data storage
Duration: state and local governments must retain records for at least two years from the creation of the record or the action involved. Unions must retain membership, referral records for one year. Private employers must retain records for at least one year; must retain one year from termination. Termination records must be retained for two years. Discrimination charge records (e.g. ADA, GINA) must be retained until the statutory period for bringing action is over or until litigation has ended.

6.6 Data access
N/A

6.7 Additional notes
N/A

7. 29 CFR § 1910.1020 Access to employee exposure and medical records

Jurisdiction
Federal regulation

7.1 Covered entities
General industry, maritime, and construction employers that make or have access to employee exposure or medical records.

7.2 Covered data
All employee exposure and medical records, and analyses of such records. Includes: environmental monitoring, biological monitoring, examination results, health questionnaires, medical opinions, and first aid information. Does not include: physical specimens, health insurance claims if maintained separately from medical records and not individually identifiable, records generated for litigation, and voluntary employee assistance programs if separate from medical records.

7.3 Data collection permissions
Mandated: employers must maintain accurate medical, exposure records for employees.

7.4 Data use
Injury surveillance: employees must provide occupational health justification when requesting records.

7.5 Data storage
Duration: records must be retained for the duration of employment and an additional 30 years.

7.6 Data access
Required employee access: employee or designated representative may request access and must be provided with access within 15 working days without cost. Employees must make exposure requests in writing and explain the occupational health justification. Employers may deny employees direct access to diagnosis of terminal illness and only share with a representative of the employee who has written consent to access the information. Employers must deidentify analysis using exposure or medical records before sharing or may deny access if deidentification is not feasible.

7.7 Additional notes
Applies to MD, VA firefighters due to state OSHA plans.

8. 29 CFR § 1904 OSHA Recordkeeping Rules

Jurisdiction
Federal regulation

8.1 Covered entities
Employers with 11 or more employees, with exceptions for low risk injuries (which must only comply with reporting for fatalities or events in which three or more employees are hospitalized). Employees on payroll regardless of status, or employees who are supervised by the employer, even if not directly employed by the employer.

8.2 Covered data
New, work-related injuries, illnesses, and fatalities that involve death, days away from work, restricted or transferred work, medical treatment (beyond first aid), loss of consciousness, or as diagnosed by a medical professional.

8.3 Data collection permissions
Mandated: employers must maintain records of recordable injuries and illnesses.

8.4 Data use
Injury surveillance: data should be collected, maintained, and analyzed to understand national occupational injury and illness trends.

8.5 Data storage
Duration: injury and illness records must be maintained for at least five years.

8.6 Data access
Required reporting: employers must report fatalities within 8 hours; serious injury (amputation, loss of eye, hospitalization) within 24 hours. Must report injuries an illnesses to OSHA if surveyed as part of annual survey.
Required aggregated sharing: employers must post a summary of injuries in the workplace for the previous year.
Required employee access: employees must be informed of the existence, location, and availability of records. Employers must provide copies of the summary of injuries to employees and their representatives upon request.

8.7 Additional notes
Applies to MD, VA firefighters due to state OSHA plans.

9. 29 CFR § 1913.10 Rules of Agency Practice and Procedure Concerning OSHA Access to Employee Medical Records

Jurisdiction
Federal regulation

9.1 Covered entities
OSHA personnel.

9.2 Covered data
Individual-level, personally identifiable employee medical information. Excludes aggregated records, death certificates, records required by 29 CFR Part 1904, exposure and biological monitoring records required by federal standards.

9.3 Data collection permissions
N/A

9.4 Data use
Injury surveillance: relates to OSHA handling of employee data for statutory purposes.
Data privacy: specifically cites privacy considerations.

9.5 Data storage
Location: records must be stored separately from other OSHA files and secured in a locked cabinet or vault (or stored securely electronically).
Duration: records must be returned or destroyed when they are no longer needed.

9.6 Data access
Limited access, sharing: OSHA representatives must make written requests to access information; these requests must be approved by the OSHA Medical Records Officer. The records must only be shared with OSHA personnel as needed for the specific intended purpose. The agency must make an annual report summarizing the number and nature of requests for access. The data should not be transferred to other agencies or the public unless required by law or approved by the Medical Records Officer.

9.7 Additional notes
The Assistant Secretary for Labor for Occupational Health and Safety will designate an OSHA Medical Records Officer responsible for approval and oversight of the handling of these records.

10. Personal Information Protection Act, Md. Code Ann. Comm. Law § 14-3504

Jurisdiction
Maryland law

10.1 Covered entities
Business entities

10.2 Covered data
Employee and former employee records; personal information including identifiers, health information (including mental health), health insurance information, and biometric data.

10.3 Data collection permissions
N/A

10.4 Data use
Data privacy: data must be stored and treated as confidential information.

10.5 Data storage
Location and security: employers must maintain reasonable security measures to protect personal information. When destroying data, must take reasonable steps to prevent unauthorized access.

10.6 Data access
Limited access: requires that data be treated as confidential. In the event of a data breach, employers must notify individuals and relevant consumer agencies.

10.7 Additional notes
Allows for right of action. Individuals can file lawsuits to recover injuries and losses. The Attorney General can impose penalties on employers who do not comply.

11. Inquiries Regarding Medical History, Md. Code Ann. Lab. & Empl. 3-701

Jurisdiction
Maryland law

11.1 Covered entities
All Maryland employers and applicants.

11.2 Covered data
Written or oral answers to questions about physical, psychiatric, or psychological disability, illness, handicap, or treatment.

11.3 Data collection permissions
Anti-discrimination: employers cannot require prospective hires to answer questions about disability unless they are directly related to work tasks. Does not prohibit a medical evaluation by a physician to assess an applicant's readiness to perform the job.

11.4 Data use
N/A

11.5 Data storage
N/A

11.6 Data access
N/A

11.7 Additional notes
N/A

12. COMAR 09.12.21 Employee Injury and Illness Records and Reports

Jurisdiction
Maryland regulation

12.1 Covered entities
All Maryland employers

12.2 Covered data
Occupational fatalities, serious injuries involving hospitalization, amputation involving bone or cartilage loss, or loss of an eye.

12.3 Data collection permissions
Presumed: employers must report fatal and serious injuries to MOSH within 8 hours (fatalities) or 24 hours (nonfatal serious injuries). Reporting must occur by phone, in person, or by electronic submission.

12.4 Data use
Injury surveillance: must report fatalities and injuries to MOSH.

12.5 Data storage
N/A

12.6 Data access
N/A

12.7 Additional notes
Serious injury definition varies slightly from federal OSHA requirements.

13. Va. Code Ann. § 8.01-413.1 Labor and Employment—Records and Recordation—Disclosure

Jurisdiction
Virginia law

13.1 Covered entities
All Virginia employers; all current and former Virginia employees.

13.2 Covered data
All employee records reflecting: dates of employment, wages or salary, job description, or injuries sustained during employment. Includes records in any format.

13.3 Data collection permissions
Presumed: assumes covered data was collected and recorded (potentially under other laws).

13.4 Data use
Injury surveillance: could be used for injury information.
Benefits: could be used to assist employee in obtaining benefits.

13.5 Data storage
N/A

13.6 Data access
Required employee access: employers must provide copies of records to current and former employees upon written request. Must provide copies within 30 days or provide notice of a delay and provide records within an additional 30 days. Employers may charge fees for copies or electronic access. Employees may subpoena records if not provided. In cases in which a medical professional indicates that providing the records would cause harm to the employee, the employer may provide access to a representative instead.

13.7 Additional notes
If the employer does not provide records or charges excess fees, a court may award damages for employee expenses, including attorney fees.

14. Va. Code Ann. § 40.1-28.7:1 Genetic Testing or Genetic Characteristics as a Condition of Employment

Jurisdiction
Virginia law

14.1 Covered entities
All Virginia employers; prospective and current Virginia employees

14.2 Covered data
Genetic tests, genetic test results, genetic characteristics.

14.3 Data collection permissions
Restrictive: employers cannot require or solicit genetic tests as a condition of employment.

14.4 Data use
Anti-discrimination: employers cannot use genetic information in employment decisions including hiring, promotion, or firing decisions. Employers may not use genetic characteristics or tests to adversely affect the terms of employment of current or prospective employees.

14.5 Data storage
N/A

14.6 Data access
N/A

14.7 Additional notes
Employees may bring action and be awarded actual or punitive damages.

15. Genetic Data Privacy, VA ST § 59.1–593 through 59.1-602

Jurisdiction
Virginia law

15.1 Covered entities
Direct to consumer (DTC) genetic testing companies, employers.

15.2 Covered data
N/A

15.3 Data collection permissions
N/A

15.4 Data use
Anti-discrimination: aimed at preventing employers from obtaining employee genetic information.

15.5 Data storage
N/A

15.6 Data access
Limited sharing: DTC companies cannot disclose consumer data to entities making decisions about employment without the consumer's express consent.

15.7 Additional notes
N/A

16. Va. Code Ann. § 65.2-900(A) Records and reports of accidents

Jurisdiction
Virginia law

16.1 Covered entities
All Virginia employers.

16.2 Covered data
Records of all employment-related injuries and deaths. Accident reports including name, employer, age, sex, wages, occupation of employee, injury date and hour, and injury nature and cause.

16.3 Data collection permissions
Mandated: employers must record all injuries and fatalities sustained in the course of employment.

16.4 Data use
Benefits: reporting to workers compensation commission and insurers.

16.5 Data storage
N/A

16.6 Data access
Required reporting: requires employers or their representatives to share injury and fatality information with workers compensation commission and their insurance carrier (if insured) within 10 days. The commission will share with the Department of Labor and Industry.

16.7 Additional notes
N/A

17. Va. Code Ann. § 40.1-51.1(D) Duties of employers

Jurisdiction
Virginia law

17.1 Covered entities
All Virginia employers.

17.2 Covered data
Information about fatal work incidents; serious work-related incidents that results in inpatient hospitalization of at least one person, amputation, or eye loss.

17.3 Data collection permissions
Presumed: assumes collection of information about fatalities and serious injuries to facilitate reporting.

17.4 Data use
Injury surveillance: fatality and injury reporting.

17.5 Data storage
N/A

17.6 Data access
Required reporting: employers must report injury and fatality information to the VA Department of Labor and Industry within 8 hours (fatal) or 24 hours (nonfatal) of incident.

17.7 Additional notes
Employers must inform employees of their rights and responsibilities under the title.

18. Va. Code Ann. § 2.2-203.2:4 Office of Data Governance and Analytics; Chief Data Officer; creation; report.

Jurisdiction
Virginia law

18.1 Covered entities
State, regional, and local public entities; public higher education institutions.

18.2 Covered data
TBD: authorizes the creation of a Chief Data Officer position to establish future rules, guidelines, and best practices for data procedures for public entities.

18.3 Data collection permissions
TBD: may result in future policymaking around data collection by public entities.

18.4 Data use
Data privacy: appears oriented towards data privacy but impact remains to be determined.

18.5 Data storage
TBD: may result in future policymaking around data storage by public entities. Specifically authorizes future policymaking around data storage and security.

18.6 Data access
TBD: may result in future policymaking around data access and sharing by public entities. Specifically authorizes policymaking around data sharing between public entities, as well as deidentification of data for research and public access.

18.7 Additional notes
2023 law authorizing broad future rules, guidelines, and best practices.

19. Presumption as to death or disability from respiratory disease, hypertension or heart disease, cancer, VA ST § 65.2–402

Jurisdiction
Virginia law

19.1 Covered entities
Virginia volunteer or career firefighters; Department of Emergency Management hazardous materials officers.

19.2 Covered data
Physical examinations conducted by qualified physicians (as prescribed by employer) for presumptive benefits. Also includes postmortem examinations of deceased employees.

19.3 Data collection permissions
Permissive: employers may request pre-employment physical examinations to find employees free of relevant diseases or conditions. May also request examinations upon employees making claims for presumptive benefits; may include tests and studies as required by the physician.

19.4 Data use
Benefits: may be used to verify the employee's health status prior to hiring or upon making a presumptive benefit claim.

19.5 Data storage
N/A

19.6 Data access
N/A

19.7 Additional notes
2023 law establishing presumption for firefighter deaths due to hypertension or heart disease, respiratory diseases, or specific cancers. Employees must comply with the employer request.

20. 16VAC25-60-80 Access to employee medical and exposure records

Jurisdiction
Virginia regulation

20.1 Covered entities
State and local public employers.

20.2 Covered data
Exposure and medical records.

20.3 Data collection permissions
Presumed: assumes collection of exposure and medical information.

20.4 Data use
Benefits: compliance with statutory, regulatory functions.
Injury surveillance: compliance with statutory, regulatory functions.

20.5 Data storage
N/A

20.6 Data access
Limited access: employers may only share data as needed for compliance. Data should not be disclosed to health professionals without the employee's written consent. Data should be shared with the Labor and Industry Commissioner only with appropriate safeguards and if necessary (regulation specifically cites privacy concerns). May only be shared as dictated in 19 CFR 1913.10.

20.7 Additional notes
Employers may request a 24 hour delay before providing records for a medical professional to be present while the records are reviewed; the Commissioner must wait so long as the employer has an affidavit that they will not modify or change the records.

21. Memorandum of Agreement, Anne Arundel County and Local 1563 IAFF (2022-2023)

Jurisdiction
Anne Arundel County Fire Department policy

21.1 Covered entities
Anne Arundel County permanent, non-probationary fire personnel, excluding leadership above the rank of Fire Captain.

21.2 Covered data
Exposure data (to hazardous materials during firefighting duties).

21.3 Data collection permissions
Presumed: refers to creation of Personal Exposure Recording Program to document exposures. Safety Committee must make recommendations regarding the program, which will be overseen by the Fire Chief.

21.4 Data use
N/A – not specified but might be for injury surveillance or benefits.

21.5 Data storage
N/A

21.6 Data access
N/A

21.7 Additional notes
N/A

22. Memorandum of Understanding between the Mayor and City Council of Baltimore and Baltimore Fire Fighters Local 734, IAFF (2022-2024)

Jurisdiction
Baltimore City Fire Department policy

22.1 Covered entities
Eligible Baltimore City Fire Department employees, including apprentices, trainees, entry level employees, and lateral entry paramedics.

22.2 Covered data
Injury reports; medical evaluations; evaluations of work-related injury, illness, or disabilities.

22.3 Data collection permissions
Mandated: injury report forms must include a box to document IDLH exposure events.
Permissive: allows for medical evaluations in general and for workplace injuries, illnesses, or disabilities.
Presumed: refers to medical status information.

22.4 Data use
Injury surveillance: injury reports must be provided to a Joint Safety and Health Committee.

22.5 Data storage
Location: medical data must be kept securely when being reviewed by an employee or his/her representative.

22.6 Data access
Limited: medical files may only be accessed by people as authorized by the Fire Chief and in the presence of a Personnel Administrator.
Required employee access: if the union requests exposure reports, the employer must provide copies within 30 days; medical status info put in an employee's medical file must be shared with employee; employees or their authorized representatives have the right to access their medical files (or authorized personnel).

22.7 Additional notes
The department stipulates that if an employee receives a medical exam, the provider must honor patient confidentiality and privacy. No description of how the department might access medical exam data.

23. Memorandum of Understanding Between the Baltimore County Administration and the Baltimore County Professional Fire Fighters Association IAFF Local 1311 (2021-2023)

Jurisdiction
Baltimore County Fire Department policy

23.1 Covered entities
Uniformed fire department classes including the rank of Fire Captain and EMS Captain.

23.2 Covered data
Medical screening data, hearing test data, medical or physical exams.

23.3 Data collection permissions
Permissive: management agrees to continue maintaining a hearing test program and to explore funding to provide comprehensive medical screenings for early cancer diagnosis and cardiac/pulmonary abnormalities. Firefighters shall receive a medical exam every 18 months and will be offered a voluntary NFPA 1582 physical.

23.4 Data use
Injury surveillance

23.5 Data storage
N/A

23.6 Data access
Limited access: medical exam or physical data will be kept private and confidential in accordance with local, state, and federal law. Specifically cites HIPAA.
Hearing test data is not explicitly addressed.

23.7 Additional notes
N/A

24. Memorandum of Understanding between the State of Maryland and the Baltimore /Washington International Airport Professional Fire Fighters Local 1742 IAFF (2022-2024)

Jurisdiction
BWI Airport Fire Department policy

24.1 Covered entities
Uniformed fire personnel, ranging from Airport Fire Fighter Trainee to Assistant Fire Marshal (Fire Prevention).

24.2 Covered data
Medically documented temporary illness or disability information.

24.3 Data collection permissions
Presumed: assumes medical evaluation or exam has taken place to document injury. Requires that employees be restored to duty if declared fit for duty by State Medical Director.

24.4 Data use
Benefits: employees may be granted up to 6 months leave without pay for a medically documented temporary illness or disability.

24.5 Data storage
N/A

24.6 Data access
N/A

24.7 Additional notes
Briefly mentions that medical leave must be documented but does not explicitly address collection of this data, how it should be stored, or who has access within the department. Only applies to leave without pay. Does not address work-related injuries, illnesses, or disabilities.

25. IAFF Local 1715 Collective Bargaining Agreement with the Mayor and City Council of Cumberland, MD (2017-2020)

Jurisdiction
Cumberland MD Fire Department policy

25.1 Covered entities
Full or part time fire department members below the rank of Captain. Excludes volunteers, fire marshal, probationary employees.

25.2 Covered data
Sick leave certification.

25.3 Data collection permissions
Permissive: requires medical documentation from a treating physician or health care provider for sick leave. The employer may not request additional information but may contact the health care provider to clarify or authenticate the certificate (after the employee is given chance to clarify).

25.4 Data use
Benefits: members must provide a department medical certificate to obtain sick leave if it is longer than one shift or the third or more instance per fiscal year. After the second instance without certification, the employee may not be paid.

25.5 Data storage
N/A

25.6 Data access
N/A

25.7 Additional notes
Allows the department to contact the medical provider who certified sick leave, but the person contacting the provider cannot be the employee's direct supervisor.

26. Agreement Between the City of Hagerstown, Maryland and IAFF Local 1605 (2018-2022)

Jurisdiction
Hagerstown Fire Department policy

26.1 Covered entities
Firefighters, apparatus operators, lieutenants, captains, and deputy fire marshals (excluding supervisors).

26.2 Covered data
Fitness for duty physical examinations.

26.3 Data collection permissions
Mandated: the department will provide (and fund) a fitness for duty physical periodically for all members (every three years for those age 30 and under, every two years for those 30-39, and every year for those 40 or older). The exam will include required tests including an EKG and cardiac stress test, labs, chest x-ray, hearing and vision tests, heart scan (baseline and at five year intervals) and mammogram as directed by personal physician. Failure to complete the physical and associated tests can result in discipline including termination.

26.4 Data use
Injury surveillance: maintaining fitness for duty.

26.5 Data storage
N/A

26.6 Data access
Required reporting: medical information that is pertinent to fitness for duty will be shared with the city's Department of Human Resources by the physician who performed the exam.

26.7 Additional notes
Does not explicitly address if and how the physical data will be stored and whether it can be shared more broadly within the department or with individual employees.

27. Agreement Between Montgomery County Career Fire Fighters Association, IAFF 1664, and Montgomery County Government (2022-2024)

Jurisdiction
Montgomery County Fire Department policy

27.1 Covered entities
Members ranging from the rank of Firefighter/Rescuer 1 to Fire/Rescue Captain. Excludes lieutenants and captains who are primarily assigned to administrative roles, including budget, internal affairs, labor relations, human resources, public information, or quality assurance.

27.2 Covered data
Sick leave documentation; service-related injury, illness, or near miss documentation; medical records; fitness records; employee assistance program records.

27.3 Data collection permissions
Mandated: to obtain sick leave, employees must provide documentation from a physician or other licensed health care provider if they are unable to work for specified periods of time. The documentation must be submitted before the end of shift following the sick leave. After four undocumented incidents, lack of documentation may result in sick leave restriction or disciplinary action. Battalion chiefs may request documentation if they believe sick leave is being abused and may require medical clearance if the employee may not be medically fit for duty. For disability leave related to occupational injuries, employees will be placed on leave after receiving certification from the on-duty Career Duty Operations Chief (and approved by the Fire Chief), and as certified by employee's physician. Upon returning to work after an occupational injury (or 15 or more days from a non-work related injury), the employee must undergo a return to work medical exam. The employer may request a medical certificate to certify FMLA leave and may request up to two additional exams. The Exercise Physiologist must keep fitness records including capacity, body composition, flexibility, muscular strength and endurance, non-medical fitness information.

27.4 Data use
Anti-discrimination: fitness data cannot be used to evaluate performance, for discipline, to evaluate workers compensation or disability claims, or take personnel action.
Benefits: sick leave documentation helps facilitate appropriate use of sick leave; medical records certify eligibility for FMLA leave.
Injury surveillance: fitness data helps maintain fitness for duty; injury and fatality information can be used by the Health and Safety Committee to make health and safety recommendations to the Fire Chief; medical exams ensure fitness for returning to work.

27.5 Data storage
Location: employee medical files must be stored securely and separately from other employee records. Fitness records must be kept securely under lock and key.

27.6 Data access

Limited access: medical documentation will be forward electronically to the Battalion Chief, who will approve sick leave. Medical records are confidential and unless the employee has provided signed authorization, must only be shared on a need-to-know basis specific county personnel including human resources, the Disability Review Panel, Disability Arbitration Board, and workers compensation administrators. The Health and Safety Committee may examine serious injury, near miss, or fatality information. The County must redact injury and fatality files to limit access to confidential information. Fitness data is confidential and may not be shared with anyone outside of the Exercise Physiologist and Peer Fitness Trainer performing the assessment. Employee assistance program information will not be communicated or released without written permission from an employee or his/her representative.

Required employee access: employees have access to their own medical files and must be notified every time an addition is made; the department will maintain a log of each time the file is accessed detailing who accessed the files and on what date (except for HR and occupational medicine personnel).

27.7 Additional notes

Includes detailed guidance on when sick leave requires documentation.

28. Collective Bargaining Agreement Between the Town of Ocean City, Maryland and Career Fire Fighter Paramedics Association of Ocean City, IAFF 4269 (2019-2022; extended to 2024)

Jurisdiction
Ocean City Fire Department policy

28.1 Covered entities
Firefighters/EMS Techs or Fire Marshals below the rank of captain. Excludes civil, casual, seasonal, part time, confidential, or supervisory employees.

28.2 Covered data
Physical fitness assessments; medical evaluations.

28.3 Data collection permissions
Permissive: the employer may require employees to undergo a physical fitness assessment and a medical evaluation annually. The Union must be notified about physical fitness assessments in advance and confer with the department about procedures and standards. The department may also require a medical exam to determine if an employee can report for modified duty, whether they have reached maximum medical improvement, or are fit for duty (the employer must fund this exam and may seek a third opinion if the treating physician and department provider disagree).

28.4 Data use
Benefits: determining whether an employee has reached maximum medical improvement and is fit to return to work.
Injury surveillance: maintaining fitness for duty.

28.5 Data storage
N/A

28.6 Data access
N/A

28.7 Additional notes
Originally effective 2019-2022, but was extended in 2020 to be effective until 2024.

29. Agreement Made By and Between Prince George's County, Maryland and IAFF 1619 (2022-2024)

Jurisdiction
Prince George's County Fire Department policy

29.1 Covered entities
Firefighters up to the rank of Battalion Chief (including Firefighter I, Firefighter Technician, Paramedic Trainees, and Firefighter Medic/Technician).

29.2 Covered data
Medical information related to an occupational injury or illness; accident information; medical physical examination information.

29.3 Data collection permissions
Presumed: if an employee is injured on the job, return to work can be dictated by release from an attending physician, release from the Medical Advisory Board, or assignment of light duty by the Medical Advisory Board. If the Fire Chief denies a request to extend disability leave, the employee may ask for the Medical Advisory Board to make a fitness for duty determination. This will be reviewed by the Disability Review Board. However, there is no explicit description of the department's collection of medical information.
Mandated: a safety officer will investigate accidents and their causes to make recommendations; the safety officer shall keep statistics and records of accidents. Employees must complete an annual medical physical exam.

29.4 Data use
Benefits: determining fitness for returning to work.
Injury surveillance: maintaining fitness for duty, understanding and preventing accidents.

29.5 Data storage
N/A

29.6 Data access
Required access: the safety officer will have access to accident information. Medical information for leave determinations might be shared with the Medical Advisory Board and/or Disability Review Board.

29.7 Additional notes
The description of leave certification and return to work inherently assumes that medical data would be collected or shared, but the contract does not specify how data would be collected or stored.

30. Collective Bargaining Agreement Between the City of Alexandria, Virginia and the IAFF 2141 (2023-2026)

Jurisdiction
Alexandria Fire Department policy

30.1 Covered entities
Firefighters from the rank of Firefighter I to Deputy Fire Marshal III, including captain and lieutenants.

30.2 Covered data
Exposure records; injury information; notice of serious injury or death; annual physical examination; audio, video, or electronic monitoring device data.

30.3 Data collection permissions
Presumed: assumes collection of serious injury or death (presumably through VA state law requiring injury and fatality recordkeeping).
Mandated: employees must provide a written statement when involved in an injury and will have the opportunity to appear before an Accident and Injury Review Board. The Department will track personal exposure data and maintain records.
Permissive: the city may review electronic monitoring device data as part of an investigation, in response to an incident or accident, or for training.

30.4 Data use
Injury surveillance: maintaining fitness for duty, understanding and preventing injuries and accidents.

30.5 Data storage
N/A

30.6 Data access
Limited access: employees may authorize the department to share notice of serious injuries or death with the union. Employees may revoke this authorization.
Required reporting/access: employees must provide injury reports. The department will share personal exposure reports with employees.

30.7 Additional notes
Does not specify how certain data will be used and authorizes broad oversight by the department; allows the department to use monitoring data for personnel or performance issues. The city has access to electronic monitoring data that might be shared within the department but this is not specified.

31. Collective Bargaining Agreement Between Arlington Professional Firefighters and Paramedics Association IAFF 2800, and Arlington County Government (2023-2026)

Jurisdiction
Arlington Fire Department policy

31.1 Covered entities
Firefighters from the rank of Firefighter/EMT to Fire/EMS Captain II.

31.2 Covered data
Video, audio, and electronic monitoring data streams; sick leave, medical donor leave, and FMLA information; exposure records; injury, illness, fatality, and accident information; medical and psychological examinations.

31.3 Data collection permissions
Mandated: employees must undergo annual medical examinations. The department will maintain exposure, medical, and injury records. The health and safety committee will review and analyze injury, accident, fatality reports.
Permissive: the department is authorized to use video, audio, and other electronic monitoring data streams, including body camera footage and apparatus recordings. The county may require documentation from a health care provider to document sick leave if the employee's sick leave has been exhausted or the employee has been disciplined within the last two years over sick leave. The county may require documentation of medical donation to approve leave. The department may conduct fitness for duty exams if leadership believe it is justified, to be conducted by a qualified physician or health care professional. Employees must comply with requests for medical records for return to work. The department may also refer an employee for a fitness evaluation.
Restrictive: the County will not require employees to answer questions about sick leave without probable cause of abuse.

31.4 Data use
Benefits: certifying sick leave or medical donor leave.
Anti-discrimination: there are additional limits on the use of electronic monitoring data; employees must receive notice through nearby postings (for audio recording) or a list of locations (for video recordings). The department cannot use the data to proactively identify policy violations but may use for internal investigations. If the department uses "look-in" capabilities (e.g. from apparatus cameras) it will try to notify employees in advance and cannot use the data for discipline or retaliation.
Injury surveillance: maintaining fitness for duty, understanding and preventing injuries, fatalities, and accidents. Electronic monitoring data may be used to improve health and safety, conduct training, and perform research or investigations. The Health and Safety Committee will examine injury and fatality information to determine causes, determine prevention, recommend care for injured firefighters, and recommend a medical testing program.

31.5 Data storage
Location: The department will maintain medical files separately from personnel files.
Duration: test results, professional records, and return to work notifications may be removed from personnel files after 30 years.

31.6 Data access
Limited access: sick leave usage information and FMLA information will be treated with same security, confidentiality as private health information under HIPAA. Only HR staff, employees or designees may review medical files. A union representative may access with authorization from an employee. The Health and Safety Committee must maintain confidentiality of medical records when reviewing medical testing programs. Employee medical history, physical exams, other lab tests from the department medical evaluation must be kept confidential. Employee Assistance Program information will be kept confidential and will not be released to anyone without the employee's written permission (unless required by law or fear that the employee will harm themselves).
Required reporting: if an employee is injured, the employer will provide copies of the notice of injury and other associated reports to the employee. The union will be notified about service-related death or injuries requiring transport to trauma, burn, specialty referral, or acute care centers; severity of injury is defined by those meriting Fire Chief notification. The Fire Chief must be notified if the employee cannot complete job functions. If a rehab program is required, the Fire Chief can require progress reports from employee. Following work-related limited duty, an employee must notify his/her supervisor and Health Wellness and Safety Officer if he/she has restrictions on return to work. The employee must also notify the battalion chief and deputy chief of restrictions.
Required employee access: employees may access medical documents in their personnel files in the presence of HR staff. Employees have access to medical and psychological exam information, occupational injury information, and exposure information; employees may make copies of these records. Employees must be given a copy of the results from their department medical evaluation.

31.7 Additional notes
Authorizes broad use of electronic monitoring explicitly for health and safety purposes; these authorizations do not include data storage, access, or sharing provisions.

Appendix 3.1 Focus group discussion questions

Current data practices		
	Data collection	• What kinds of personal information do you provide to the department right now? [personal identifiers, health information, injury reporting] • Are there things that you don't want to share with management? What about the union? Why? • Do you collect your own information about things like injuries? [e.g. NFORS]
	Data use	• What is this information used for? [compliance, research, safety, workers comp, human resources]
	Data sharing	• Who do you think this information is shared with in the department? • What about outside of the department? [government, research, contractors]

Appendix 3.2 Focus group exit survey

Participant number:

1. What is your age?

2. Do you identify as:
    a. Female
    b. Male
    c. Nonbinary/other

3. Do you identify as (select all that apply):
    a. Asian
    b. Black
    c. White
    d. Hispanic or Latino/Latina
    e. Native American or Alaska Native
    f. Other

4. Do you use a fitness tracker (e.g. a FitBit)?
    a. Yes
    b. No

5. Do you use a smartwatch (e.g. an Apple watch)?
    a. Yes
    b. No

6. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?
    a. Yes
    b. No
    c. Not sure (please elaborate):

7. Do you document your exposures using an app like NFORS or through your own recordkeeping?
    a. Yes – I use an app like NFORS
    b. Yes – I use my own recordkeeping system
    c. No

Appendix 3.3 Union leader interview questions

Before we begin our discussion, I want to ask you a few demographic and background questions:

1. What is your age?
2. What is your gender?
3. What is your race/ethnicity?
4. What is your rank?
5. How many years of experience do you have in the fire service?
6. Do you use a fitness tracker (e.g. a FitBit)?
7. Do you use a smartwatch (e.g. an Apple watch)?
8. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?

Current data practices		
	Data collection	• What types of workforce data does the union collect right now? (e.g. injury data) • Does the union encourage members to collect their own injury data? (e.g. NFORS) • Do you know what types of workforce data the department collects? • How much time or resources do you devote to mandatory reporting? What about voluntary data collection? • Are there any challenges in collecting or storing this data? • What kinds of software or technology do you use to manage this data? • Have you received any training or guidance on data privacy (e.g. what kind of data you can collect from staff, data storage and security)?
	Data use	• How does the union use this data? • How would you say the department currently uses safety-related data (e.g. injury data)? • What about other types of information?
	Data sharing	• Who is that data shared with in the union? The department? What about outside of the department? • Do you have partnerships with any professional societies or researchers?

Appendix 3.4 Department leader interview questions

Before we begin our discussion, I want to ask you a few demographic and background questions:

1. What is your age?
2. What is your gender?
3. What is your race/ethnicity?
4. What is your rank?
5. How many years of experience do you have in the fire service?
6. Do you use a fitness tracker (e.g. a FitBit)?
7. Do you use a smartwatch (e.g. an Apple watch)?
8. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?

Current data practices		
	Data collection	• What types of workforce data do you collect right now for reporting purposes or for a safety initiative? • How much time or resources do you devote to mandatory reporting? What about voluntary data collection? • Are there any challenges in collecting or storing this data? • What kinds of software or technology do you use to manage this data? • Have you received any training or guidance on data privacy (e.g. what kind of data you can collect from staff, data storage and security)?
	Data use	• How would you say the department currently uses safety-related data (e.g. injury data)? • What about other types of information?
	Data sharing	• Who is that data shared with in the department? What about outside of the department? Do you have partnerships with any professional societies or researchers?

Appendix 3.5 National leader interview questions

Before we begin our discussion, I want to ask you a few demographic and background questions:

1. What is your age?
2. What is your gender?
3. What is your race/ethnicity?
4. What is your rank?
5. How many years of experience do you have in the fire service?
6. Do you use a fitness tracker (e.g. a FitBit)?
7. Do you use a smartwatch (e.g. an Apple watch)?
8. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?

Current data practices		
	Data collection	• What types of safety or injury data do you collect right now? • How much time or resources do you devote to mandatory reporting? What about voluntary data collection? • Are there any challenges in collecting or storing this data? • Have you received any training or guidance on data privacy (e.g. what kind of data you can collect from firefighters or departments, data storage and security)?
	Data use	• How do you use this safety-related data (e.g. injury data)? • What about other types of information?
	Data sharing	• Who is that data shared with in your organization? What about outside of your organization (e.g. departments, other fire service organizations, government)? • Do you have partnerships with any professional societies or researchers?

Appendix 3.6 Codebook

CODE	DEFINITION
Nature of data	**Placeholder - do not code**
exposure data	Text describing data collection on exposure to toxins (e.g. CO2, smoke, PFAS). Apply for data collection, use, and sharing; will often be double coded.
injury and fatality data	Text describing data collection on injury or fatalities. Apply for data collection, use, and sharing; will often be double coded.
physical health/medical data	Text describing data collection on exercise, diet, biomarker, physicals, cancer, heart disease, sleep. Apply for data collection, use, and sharing; will often be double coded.
mental/behavioral health data	Text describing data collection on suicide, mental health
underrepresented minority data	Text describing data collected on specific groups (e.g. FF census, harassment/bullying, reproductive health)
HR data	Text describing data collection on personnel issues (e.g. recruitment, retention, performance). Apply for data collection, use, and sharing; will often be double coded.
Data collection	**Placeholder - do not code**
current data collection	Text describing current data collection practices
data collection uncertainty	Text capturing uncertainty about what kinds of data are currently or could be collected
future data collection/data gaps	Text describing preferences regarding future data collection and gaps in current data collection
no data gaps	Text describing little or no need for more data collection
conditions for data collection	Text describing conditions that should be in place for data collection (e.g. voluntary, consent)
data collection challenges	Text describing barriers to high quality data collection (administrative burden, data quality, costs, tech)
self-tracking	Text describing efforts to track one's own data (using NFORS or something else)
risk calculus	Text describing the role of risk in determining acceptable data collection (privacy/safety tradeoff)
Data use	**Placeholder - do not code**
health and safety practices	Text describing how data is being used or could be used to improve health and safety through training, new practices and procedures
responding to calls	Text describing using data to improve safety when on a call, IDLH
facilitating benefits	Text describing using data to help ensure access to workers comp, presumptive benefits
policy development	Text describing using data to inform policymaking, building codes, professional standards (e.g. NFPA)

research	Text describing using data for research
job repercussions	Text capturing concerns that data will be used to limit job tasks or fire someone
discrimination	Text capturing concerns that data will be used to discriminate
improving DEI	Text describing the potential for data to enhance DEI efforts. Include text describing data as a tool to protect, improve diversity and equity
improving recruitment, retention	Text describing the potential for data to enhance recruitment, retention efforts
commercial use	Text capturing opposition to or limits on commercial use of data
data linkages	Text capturing discussion of data linkages (explicitly or implicitly)
data use uncertainty	Text describing uncertainty about how data is currently used or could be used
data training	Text describing data/privacy training respondent has received (or lack thereof)
Data sharing	**Placeholder - do not code**
sharing concerns	Text capturing concerns (personally or from others) about data sharing
sharing support	Text capturing support (personally or from others) for data sharing
trust	Text capturing the role of trust in willingness to share information within a department or with outside entities
accessing your own data	Text capturing the value of having access to your own data, for benefits, health, or any purpose. Can double code with "data use" codes like "facilitating benefits" if relevant
aggregated data sharing	Text describing views on sharing aggregated, deidentified data (e.g. research findings)
data sensitivity	Text describing the sensitivity of sharing certain types of data (e.g. mental health or behavioral health data)
sharing within department	Text describing views on sharing data within the department (identifiable and deidentified), including current data access within the department
external sharing/collaboration	Text describing sharing data outside of the department (also include collaborations that are not explicitly data focused)
no sharing concerns	Text describing no preferences or concerns about data sharing
data sharing uncertainty	Text capturing uncertainty about how data is currently shared or how it could be shared
Data perceptions	**Placeholder - do not code**
paradigm shift	Text describing the need for a paradigm shift in the fire service towards valuing data
tool for protecting our own	Text reflecting the value of data to protect firefighters, support future generations

tool for funding	Text describing the role of data in understanding financial impacts (e.g. of injury), advocating for funding
empowering firefighters	Text describing using data to empower firefighters to understand their health, make healthy sleep, exercise, diet decisions
data liability	Text describing the view that data creates liability (to secure data itself and responsibility for health issues)
data utilization and access	Text describing underutilization or how to best utilize data, or accessing existing data (e.g. only valuable if you use it, double edged sword revealing negative trends)
data purpose	Text describing the need to collect, use, share data with a specific purpose or intent in mind
privacy preconceptions	Text capturing previous consideration of privacy issues (or lack thereof)
HIPAA	Text referencing HIPAA as an example (include confusion about HIPAA. Double code with "data literacy" if misinterpreting HIPAA)
importance of education	Tech describing the importance of education on data and/or tech. Can apply both in general and in reference to new data collection
Fire service	**Placeholder - do not code**
community relationship	Text describing department-community relationships, including community-facing data, the department looking like the community. Does not need to include data
union relationship	Text describing union-management relationship, including tension with the union
identity	Text describing firefighting as an identity, fear of losing identity
change is hard	Text capturing change in the fire service, challenges of introducing changes
generational divide	Text describing generational divides in the fire service
firefighter empowerment	Text describing ways to empower firefighters or the importance of empowerment
career v. volunteer	Text describing differences between career and volunteer firefighters
fire service/department culture	Text capturing descriptions of how department culture affects data privacy practices or views

Appendix 4.1 Firefighter health and safety wearable technologies and associated data

Type of device[3,55,56]	**Example types of data collected**[3,55,56]	**Example use case(s)** [3,55,56]
Biometric sensors attached to PPE or individual firefighter	• Heart rate • Blood pressure • Skin or core temperature • Motion • Respiratory rate	• Used to evaluate firefighter capacity on incidents and inform rest cycles • Used to identify firefighters in distress on a fireground • Data analyzed after incidents to understand health, fitness trends
Exposure sensors (e.g. dosimeter, particulate sensors) integrated into PPE or as handheld devices	• Heat (environmental) • Chemicals • Fire smoke • Gases • Specific toxins (e.g. benzene, carbon monoxide, formaldehyde, hydrogen chloride, sulfur dioxide)	• Used in structure fire to anticipate flashover conditions, alert firefighters to evacuate before flashover occurs • Data analyzed after incidents to evaluate exposure limits, staffing, and rest cycles
Location tracker (e.g. GPS or RFID) attached to PPE or individual firefighter	• Location data	• Used on fireground by incident commander and rapid intervention team to locate a firefighter who is injured or trapped in a structure fire

Appendix 4.2 Focus group discussion questions

There is lots of interest in using new technologies like a wearable device to help improve health and safety. This could involve asking firefighters to wear a device to collect biometric information or location data. This information could be used while on a call, to conduct research, improve health and safety practices, and inform firefighters about their health. I want to ask about your views on wearables in a few different scenarios.

Scenario 1: Safety biometrics
Let's talk about a scenario. In this one, let's imagine that the department is implementing a new biometric vest to be worn responding to calls. Wearing the vest will be mandatory as part of your PPE. It will collect data on your heart rate, blood pressure, temperature, blood oxygen levels, and location. The data will be used in real time during calls. For instance, an incident commander will have access to the data and can use it to make decisions on calls. It will also be used to inform the department's health and safety tracking, prevention, and training. The individual data will be shared with leaders who are managing calls, and will be shared with department leaders responsible for health and safety. It will be shared in an aggregated, de-identified way with overall department leadership. You would have access to your individual data.

- Would you be in favor of this or not in favor? Why/why not?
- Do you have any concerns? Probe: data privacy, sharing
- Would you want access to your own data? How would you use it?
- How would you feel about sharing your data with leaders in the department?
- How would you feel about sharing your data with researchers?
- How would you feel about sharing your data with government officials (e.g. USFA)?
- What if participation was voluntary?

Scenario 2: Exposures
Let's imagine a different scenario. In this one, let's imagine that the department is implementing new PPE that includes wearable sensor devices on the outside of your gear. Wearing the sensors will be mandatory as part of your PPE when responding to calls. It will collect data on your exposure to things like CO2 and carbon monoxide, particulates, and other toxins. It will also track external temperature and your location. The data will be used in real time during calls. For instance, an incident commander will have access to the data and can use it to make decisions on calls. It will also be used to inform the department's health and safety tracking, prevention, and training. The individual data will be shared with leaders who are managing calls, and will be shared with department leaders responsible for health and safety. It will be shared in an aggregated, de-identified way with overall department leadership. You would have access to your individual data.

- Would you be in favor of this or not in favor? Why/why not?
- Do you have any concerns? Probe: data privacy, sharing
- Would you want access to your own data? How would you use it?
- How would you feel about sharing your data with leaders in the department?

- How would you feel about sharing your data with researchers?
- How would you feel about sharing your data with government officials (e.g. USFA)?
- What if participation was voluntary?

Scenario 3: Wellness biometrics

To start, let's imagine that the department is starting a new health and wellness program. They will offer all firefighters a wearable device to track health metrics. The device would be similar to an Apple watch and would collect information about your: heart rate, blood oxygen levels, movement, noise exposures, falls, and sleep. Participation would be voluntary. You would have access to all of your data. You could opt into sharing your data with health and safety staff. Department leadership and researchers would have access to de-identified, aggregated data.

- Would you want to participate? Why/why not?
- If you participated, how would you use the information from the watch?
- Do you have any concerns? Probe: data privacy, sharing
- How would you feel about sharing your data with leaders in the department?
- How would you feel about sharing your data with researchers?
- How would you feel about sharing your data with government officials (e.g. USFA)?

Appendix 4.3 Focus group exit survey

Participant number:

1. What is your age?

2. Do you identify as:
    a. Female
    b. Male
    c. Nonbinary/other

3. Do you identify as (select all that apply):
    a. Asian
    b. Black
    c. White
    d. Hispanic or Latino/Latina
    e. Native American or Alaska Native
    f. Other

4. Do you use a fitness tracker (e.g. a FitBit)?
    a. Yes
    b. No

5. Do you use a smartwatch (e.g. an Apple watch)?
    a. Yes
    b. No

6. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?
    a. Yes
    b. No
    c. Not sure (please elaborate):

7. Do you document your exposures using an app like NFORS or through your own recordkeeping?
    a. Yes – I use an app like NFORS
    b. Yes – I use my own recordkeeping system
    c. No

Appendix 4.4 Union leader interview questions

Before we begin our discussion, I want to ask you a few demographic and background questions:

1. What is your age?
2. What is your gender?
3. What is your race/ethnicity?
4. What is your rank?
5. How many years of experience do you have in the fire service?
6. Do you use a fitness tracker (e.g. a FitBit)?
7. Do you use a smartwatch (e.g. an Apple watch)?
8. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?

Data and privacy preferences		
	Data collection	• Are there types of information you would like to have but don't currently have access to? • Are there types of information that you don't think the department should have access to? • How would you feel about using technology like a wearable device to help collect and store safety-related data? Do you anticipate any challenges? [acceptance, privacy, logistical]
	Data use	• What would you use that data for? [research partnerships, recruitment, reporting]
	Data sharing	• Would you want to share this information with entities outside of the union? [department, researchers, the government, contractors, tech companies]

Appendix 4.5 Department leader interview questions

Before we begin our discussion, I want to ask you a few demographic and background questions:

1. What is your age?
2. What is your gender?
3. What is your race/ethnicity?
4. What is your rank?
5. How many years of experience do you have in the fire service?
6. Do you use a fitness tracker (e.g. a FitBit)?
7. Do you use a smartwatch (e.g. an Apple watch)?
8. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?

Data and privacy preferences		
	Data collection	• Are there types of information you would like to have but don't currently have access to? • What types of information might help improve your safety programs or reduce injuries? • How would you feel about using technology like a wearable device to help collect and store this data? Do you anticipate any challenges? [acceptance, privacy, logistical]
	Data use	• What would you use that data for? [research partnerships, recruitment, reporting]
	Data sharing	• Who do you think it would be helpful to share this information with? [researchers, the government, contractors, tech companies]

Appendix 4.6 National leader interview questions

Before we begin our discussion, I want to ask you a few demographic and background questions:

1. What is your age?
2. What is your gender?
3. What is your race/ethnicity?
4. What is your rank? (if applicable)
5. How many years of experience do you have in the fire service? (if applicable)
6. Do you use a fitness tracker (e.g. a FitBit)?
7. Do you use a smartwatch (e.g. an Apple watch)?
8. Do you use social media platforms (e.g. Twitter, Facebook, or Instagram)?

Data and privacy preferences		
	Data collection	• Are there types of information you would like to have but don't currently have access to? • What types of information might be most helpful for improving safety? • How would you feel about using technology like a wearable device to help collect and store this data? Do you anticipate any challenges? [acceptance, privacy, logistical]
	Data use	• What would you use that data for? [research partnerships, reporting]
	Data sharing	• Who do you think it would be helpful to share this information with? [firefighters, departments, researchers, the government, contractors, tech companies]

Appendix 4.7 Codebook

CODE	DEFINITION
Nature of data	Placeholder - do not code
exposure data	Text describing data collection on exposure to toxins (e.g. CO2, smoke, PFAS). Apply for data collection, use, and sharing; will often be double coded.
injury and fatality data	Text describing data collection on injury or fatalities. Apply for data collection, use, and sharing; will often be double coded.
physical health/medical data	Text describing data collection on exercise, diet, biomarker, physicals, cancer, heart disease, sleep. Apply for data collection, use, and sharing; will often be double coded.
mental/behavioral health data	Text describing data collection on suicide, mental health
underrepresented minority data	Text describing data collected on specific groups (e.g. FF census, harassment/bullying, reproductive health)
HR data	Text describing data collection on personnel issues (e.g. recruitment, retention, performance). Apply for data collection, use, and sharing; will often be double coded.
Wearables	Placeholder - do not code.
supportive - health and safety	Text describing support (personally or from others) for wearables for health and safety purposes (and reasons why)
supportive - responding to calls	Text describing support (personally or from others) for wearables used while responding to calls (e.g. for incident commander, IDLH)
DEI benefits	Text describing potential DEI-related benefits of wearable tech (e.g. understanding health risks)
automated data collection	Text describing the benefits or drawbacks of automated data collection (e.g. data quality, real time data)
concerned - job repercussions	Text capturing concerns about wearable data negatively impacting job status
concerned - logistics, cost, access	Text capturing concerns about the logistical challenges associated with wearable tech (e.g. costs, maintaining equipment, access, security)
strategies for buy in	Text describing strategies for increasing support for wearable tech, including tech novelty
Data perceptions	Placeholder - do not code
paradigm shift	Text describing the need for a paradigm shift in the fire service towards valuing data
tool for protecting our own	Text reflecting the value of data to protect firefighters, support future generations
tool for funding	Text describing the role of data in understanding financial impacts (e.g. of injury), advocating for funding

empowering firefighters	Text describing using data to empower firefighters to understand their health, make healthy sleep, exercise, diet decisions
data liability	Text describing the view that data creates liability (to secure data itself and responsibility for health issues)
data utilization and access	Text describing underutilization or how to best utilize data, or accessing existing data (e.g. only valuable if you use it, double edged sword revealing negative trends)
data purpose	Text describing the need to collect, use, share data with a specific purpose or intent in mind
privacy preconceptions	Text capturing previous consideration of privacy issues (or lack thereof)
HIPAA	Text referencing HIPAA as an example (include confusion about HIPAA. Double code with "data literacy" if misinterpreting HIPAA)
importance of education	Tech describing the importance of education on data and/or tech. Can apply both in general and in reference to new data collection
Fire service	Placeholder - do not code
community relationship	Text describing department-community relationships, including community-facing data, the department looking like the community. Does not need to include data
union relationship	Text describing union-management relationship, including tension with the union
identity	Text describing firefighting as an identity, fear of losing identity
change is hard	Text capturing change in the fire service, challenges of introducing changes
generational divide	Text describing generational divides in the fire service
firefighter empowerment	Text describing ways to empower firefighters or the importance of empowerment
career v. volunteer	Text describing differences between career and volunteer firefighters
fire service/department culture	Text capturing descriptions of how department culture affects data privacy practices or views

Curriculum Vitae

RACHEL JAMIE MICHI TOPAZIAN

Contact

Johns Hopkins Bloomberg School of Public Health
Department of Health Policy and Management
624 N. Broadway, Rm. 597
Baltimore, MD 21205

email: rtopazi1@jhu.edu
pronouns: she/her/hers

Education

2020-2024 (expected) **Doctor of Philosophy,** Health Policy and Management
Johns Hopkins Bloomberg School of Public Health, Baltimore, MD
Concentration: Health and Public Policy
Dissertation (in progress): Data privacy in the fire service: the regulatory environment, firefighter preferences, and leadership perspectives

2010-2013 **Bachelor of Arts**, Philosophy (*magna cum laude*)
Wheaton College, Wheaton IL
Minor: English

Professional Experience

2020-present **Graduate Research Assistant**
Johns Hopkins Bloomberg School of Public Health, Baltimore, MD

- *Describing trends in harassing behavior towards public health researchers: a survey* (PIs: Tara Kirk Sell and Beth Resnick)
- *Understanding the factors influencing federal regulatory decision making* (PIs: Beth McGinty and Shelley Hearne)
- *The role of permit-to-purchase in the primary prevention of multiple forms of violence* (PI: Cassandra Crifasi)
- *Violent crime review commission to prevent gun violence in Hampton, VA* (PI: Cassandra Crifasi)
- *The Johns Hopkins COVID-19 civic life and public health survey* (PIs: Colleen Barry, Beth McGinty, Hahrie Han, and Adam Seth Levine)

2016-2020 **Multiple Roles**
Managing Research Director (2020)
Senior Research Director (2019-2020)
Research Director (2017-2018)
Health Policy Analyst (2016-2017)
National Journal, Washington D.C.

2014-2016 **Research Program Coordinator**
Johns Hopkins Berman Institute of Bioethics, Baltimore, MD

Funding

2023-2024 **Data privacy perspectives in the context of workplace safety** (T42 OH0008428)

Pilot Project Research Training Award
Johns Hopkins Education and Research Center for Occupational Safety and Health
National Institute for Occupational Safety and Health
Amount: $8,000
Role: Principal Investigator

2020-2023 **Occupational Injury Epidemiology and Prevention Training Grant** (T42 OH0008428)
National Institute for Occupational Safety and Health
Amount: 100% salary support, tuition
PI: Ram Ramachandran
Role: Pre-doctoral Trainee

Publications

Peer-Reviewed Journal Articles

1. Webster DW, Richardson J, Meyerson N, St. Vil C, **Topazian R**. Research on the Effects of Hospital-Based Violence Intervention Programs: Observations and Recommendations. *The ANNALS of the American Academy of Political and Social Science*. Published online, 2023. doi:10.1177/00027162231173323

2. **Topazian RJ**, McGinty EE, Han H, Levine AS, Anderson KE, Presskreischer RE, Barry CL. US Adults' Beliefs About Harassing or Threatening Public Health Officials During the COVID-19 Pandemic. *JAMA Network Open*. 2022;5(7):e2223491. doi:10.1001/jamanetworkopen.2022.23491

3. **Topazian RJ**, Levine AS, McGinty EE, Barry CL, Han H. The influence of civic associations and exposure to ideological heterogeneity on public views on mask wearing and social distancing. *Preventive Medicine*. 2022;160:107098. doi:10.1016/j.ypmed.2022.107098

4. **Topazian RJ**, Levine AS, McGinty EE, Barry CL, Han H. Civic engagement and psychological distress during the COVID-19 pandemic. *BMC Public Health*. 2022;22(1):869. doi:10.1186/s12889-022-13289-4

5. Hatton CR, **Topazian RJ**, Barry CL, McGinty EE, Levine AS. Predictors of Public Support for Social Safety Net Policy During the COVID-19 Pandemic. *American Journal of Preventive Medicine*. 2022;63(1):77-84. doi:10.1016/j.amepre.2022.01.013

6. **Topazian RJ**, Hatton CR, Barry CL, Levine AS, McGinty EE. Public support for U.S. social safety net policies throughout the COVID-19 pandemic. *Preventive Medicine*. 2022;154:106873. doi:10.1016/j.ypmed.2021.106873

7. Dukhanin V, **Topazian R**, DeCamp M. Metrics and Evaluation Tools for Patient Engagement in Healthcare Organization- and System-Level Decision-Making: A Systematic Review. *Int J Health Policy Manag*. 2018;7(10):889-903. doi:10.15171/ijhpm.2018.43

8. Beach MC, **Topazian R**, Chan KS, Sugarman J, Geller G. Climate of Respect Evaluation in Intensive Care Units: Development of an Instrument (CORE-ICU). *Crit Care Med*. 2018;46(6):e502-e507. doi:10.1097/CCM.0000000000003069

9. Weinfurt KP, Bollinger JM, Brelsford KM, Bresciani M, Lampron Z, Lin L, **Topazian RJ**, Sugarman J. Comparison of Approaches for Notification and Authorization in Pragmatic Clinical Research Evaluating Commonly Used Medical Practices. *Med Care*. 2017;55(11):970-978. doi:10.1097/MLR.0000000000000762

10. Carrese JA, Geller G, Branyon ED, Forbes LK, **Topazian RJ**, Weir BW, Khatib O, Sugarman J. A Direct Observation Checklist to Measure Respect and Dignity in the ICU. *Critical Care Medicine*. 2017;45(2):263-270. doi:10.1097/CCM.0000000000002072

11. **Topazian R**, Bollinger J, Weinfurt KP, Dvoskin, R, Mathews D, Brelsford K, DeCamp M, Sugarman J. Physicians' perspectives regarding pragmatic clinical trials. *J Comp Eff Res*. 2016;5(5):499-506. doi:10.2217/cer-2016-0024

12. Geller G, Branyon ED, Forbes LK, **Topazian RJ**, Weir BW, Carrese JA, Beach MC, Sugarman J. ICU-RESPECT: An index to assess patient and family experiences of respect in the intensive care unit. *Journal of Critical Care*. 2016;36:54-59. doi:10.1016/j.jcrc.2016.06.018

13. Weinfurt KP, Bollinger JM, Brelsford KM, Crayton TJ, **Topazian RJ**, Kass NE, Beskow LM, Sugarman J. Patients' views concerning research on medical practices: Implications for consent. *AJOB Empirical Bioethics*. 2016;7(2):76-91. doi:10.1080/23294515.2015.1117536

14. Pasalic D, Gazelka HM, **Topazian RJ**, Bucchalter LC, Ottenberg AL, Webster TL, Swetz KM, Mueller PS. Palliative Care Consultation and Associated End-of-Life Care After Pacemaker or Implantable Cardioverter-Defibrillator Deactivation. *Am J Hosp Palliat Care*. 2016;33(10):966-971. doi:10.1177/1049909115595017

15. Ottenberg AL, Mueller PS, **Topazian RJ**, Kaufman S, Swetz KM. "It's Not Broke, So Let's Not Try to Fix It": Why Patients Decline a Cardiovascular Implantable Electronic Device. *Pacing Clin Electrophysiol*. 2014;37(10):1306-1314. doi:10.1111/pace.12433

16. Ottenberg AL, Cook KE, **Topazian RJ**, Mueller LA, Mueller PS, Swetz KM. Choices for patients "without a choice": Interviews with patients who received a left ventricular assist device as destination therapy. *Circ Cardiovasc Qual Outcomes*. 2014;7(3):368-373. doi:10.1161/CIRCOUTCOMES.113.000660

17. **Topazian RJ**, Hook CC, Mueller PS. Duty to speak up in the health care setting a professionalism and ethics analysis. *Minn Med*. 2013;96(11):40-43.

Teaching Experience

Teaching Assistantships, Johns Hopkins Bloomberg School of Public Health

2024	**Public Health and the Law**, Jon Vernick
2023	**Social Policy for Vulnerable Population in the U.S.**, Alene Kennedy-Hendricks
	Issues in Injury and Violence Prevention, Jon Vernick
	Public Health Policy, Joshua Sharfstein
	Research and Evaluation Methods for Health Policy, Cassandra Crifasi
	Fundamentals of Health Policy and Management, Conan Dickson
2022	**Social Policy for Vulnerable Population in the U.S.**, Alene Kennedy-Hendricks
	Issues in Injury and Violence Prevention, Jon Vernick
	Research and Evaluation Methods for Health Policy, Cassandra Crifasi
	Fundamentals of Health Policy and Management, Conan Dickson
2021	**Social Policy for Vulnerable Populations in the U.S.**, Beth McGinty

Guest Lectures

2019, 2018	**Practical Policymaking Considerations,** SUNY Upstate Medical University. Syracuse, NY.

Honors and Awards

2020-present	NIOSH Occupational Injury Epidemiology and Prevention Training Grant (award number T42 OH0008428)
2023-2024	NIOSH Johns Hopkins Education and Research Center for Occupational Safety and Health Pilot Project Research Training Award (award number T42 OH0008428)
2023-2024	Susan P. Baker Scholarship in Injury Prevention and Control, Johns Hopkins Bloomberg School of Public Health
2023-2024	Center for Qualitative Studies in Health and Medicine Dissertation Enhancement Award, Johns Hopkins Bloomberg School of Public Health

Professional Activities

Academic Service

2022-2023	Doctoral Student Representative, Public Health Threats and Harassment Taskforce, Johns Hopkins Bloomberg School of Public Health
2021-2022	Secretary, Department of Health Policy and Management Student Coordinating Committee

Society Membership

2023-present	The Society for Advancement of Violence and Injury Research
2022-present	Association for Public Policy Analysis and Management

Presentations

Scientific Meeting Poster Presentations

1. **Americans' beliefs about harassing or threatening public health officials during the COVID-19 pandemic.** Association for Public Policy and Management Fall Conference, Washington D.C. Poster presentation. Fall 2022.

2. **Network analysis of pharmaceutical pricing policy proposals.** AcademyHealth National Health Policy Conference, Washington D.C. Poster presentation. Fall 2017.

Invited Seminars

1. **Mapping the stakeholders behind 2020 presidential candidates**. Professional Women in Advocacy Conference, Washington D.C. Spring 2019.