Preparing for compounding crises: Staff shortages and cyber-attack vulnerability in the era of COVID-19

Received (in revised form): 15th July, 2022

Joshua Klindienst*

Emergency Physician, US Acute Care Solutions, USA

Shant Ayanian**

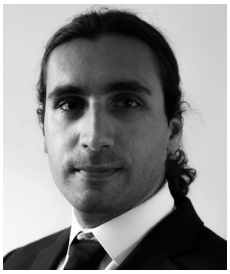
Assistant Professor of Medicine, Alix School of Medicine, Mayo Clinic, USA

Jeff Schlegelmilch†

Research Scholar and Director, National Center for Disaster Preparedness, Columbia University, USA

Hana Akselrod††

Assistant Professor of Medicine, George Washington University, USA



Joshua Klindienst

Shant Ayanian

***Joshua Klindienst** is an emergency physician at multiple clinical sites in the state of Maryland. Outside the emergency room his interests include physician education, event medicine, emergency planning and disaster response. He is also passionate about adaptation, teamwork and responsive patient care. Joshua is a member of the Maryland Task Force-1 Urban Search and Rescue team and has served as assistant medical director for the Wells Fargo Championship. He received his medical degree from the NYU School of Medicine.*

***Shant Ayanian** is an assistant professor of medicine at the Alix School of Medicine at the Mayo Clinic. He received his medical degree from the American University of Beirut, and master's degrees in bioinformatics and data science from the George Washington University. His research interests include the use of artificial intelligence systems with electronic medical records, the integration of genomics data with clinical data, and the study of methodologies for informatics process integration.*

***Jeff Schlegelmilch** is Director of the National Center for Disaster Preparedness at Columbia University. His expertise includes public health preparedness, community resilience and the integration of private and public sector capabilities. He is the author of 'Rethinking Readiness: A Brief Guide to Twenty-First-Century Megadisasters' published by Columbia University Press. He holds a Master of Public Health degree in health policy and management from UMass Amherst, and a master of business administration degree from Quinnipiac University.*

***Hana Akselrod** is an assistant professor of medicine at the George Washington University (GW) School of Medicine and Health Sciences. Since 2020 she has played a key part in pandemic response, including roles as clinical trials investigator, as co-director of the GW COVID-19 Intelligence Unit and GW COVID-19 Recovery Clinic, and as the GW Medical Faculty Associates COVID-19 Response Lead. Prior to this, her research interests focused on infectious disease epidemiology*

**US Acute Care Solutions, UPMC Western Maryland, 12500 Willowbrook Road, Cumberland, MD 21502, USA*
E-mail: joshklindienstmd@gmail.com

***Alix School of Medicine, 200 First Street SW, Rochester MN 55905, USA*
Tel: +1 507 773 3589;
E-mail: ayanian.shant@mayo.edu

†National Center for Disaster Preparedness (NCDP), Columbia University Earth Institute, 475 Riverside Drive, Suite 401, New York, NY 10115, USA
E-mail: js4645@columbia.edu

††George Washington University Medical Faculty Associates, 2150 Pennsylvania Ave. NW, Suite 8-436, Washington, DC 20037, USA
Tel: +1 202 741 2234;
E-mail: hakselrod@guu.edu

Journal of Business Continuity & Emergency Planning
Vol. 16, No. 2, pp. 103–120

Jeff Schlegelmilch

Hana Akselrod

and public health systems response. She is a founding member of the GW Climate and Health Institute. She attended the Mount Sinai School of Medicine and the Yale School of Public Health.

Abstract

In 2020, while the USA was experiencing successive waves of COVID-19, Universal Health Services experienced a major cyber attack that crippled electronic systems in over 200 hospitals, including a major academic medical centre that was playing a key regional role in COVID-19 care and clinical trials. This paper discusses the impact of the attack on clinical operations, informatics, research and teaching, contextualising the case study within more wide-scale trends driving the rise in cyber attacks on healthcare systems. The compounding relationships between COVID-19, healthcare workforce depletion and cyber-security vulnerabilities form the framework of the discussion and action plan. Commitments to institutional best practices, large-scale investments in infrastructure, and above all increasing support for the critical human actors carrying out the work, are urgently needed to secure the healthcare system against these destabilising threats. Within this context, this paper argues that information security in the healthcare sector must be reimagined and integrated with greater support for the needs of frontline healthcare workers.

Keywords: COVID-19, cyber attacks, healthcare sector, information security

INTRODUCTION

In the USA the demand for medical resources is ever-increasing. Pre-dating the COVID-19 crisis, these conditions have been attributed to a growing, ageing population with higher medical complexity as advances in treatment and technology now allow individuals with chronic illnesses to live longer.[1] Emergency department (ED) visits reflect this trend, outpacing population growth for two decades and increasing by 11 per cent between 2008 and 2018 (ie prior to the mass disturbances driven by the COVID-19 pandemic).[2] Individuals seek care in the ED for a wide variety of reasons, including shortage of accessible physicians and services in other settings (including primary, mental health and substance use care), lack of insurance coverage, growing economic disparities and systemic under-investment in disease prevention, resulting in over-reliance on frontline care, even as powerful economic drivers channel this care into increasingly consolidated medical systems.[3,4] The rise in demand has not been matched with a commensurate rise in supply, with projection models accurately anticipating nurse, physician and advanced-practice provider shortfalls for the past three decades; static residency class sizes have constrained the supply of newly trained physicians, even as the healthcare workforce has been ageing alongside the general population and veteran practitioners retiring.[5–7] These shortage conditions were exacerbated by the arrival of the COVID-19 pandemic, hastening existing burnout and attrition in a time of increased need.

Further, the level of funding available for healthcare preparedness has been inconsistent and generally falling. The primary healthcare preparedness grant, the Hospital Preparedness Program, peaked shortly after the 9/11 attacks, at nearly US$500m per annum. Preparedness funding subsequently dropped by nearly half that amount (about US$229m), recovering only slightly to the current level of US$280m annually (Figure 1). This amount is far below the US$500m level recommended at the programme's commencement.[8–10] There have been intermittent funding surges for event-specific Congressional appropriations, such as responses to epidemic influenza H1N1 (2009), Ebola and Zika virus, among others, but such direct

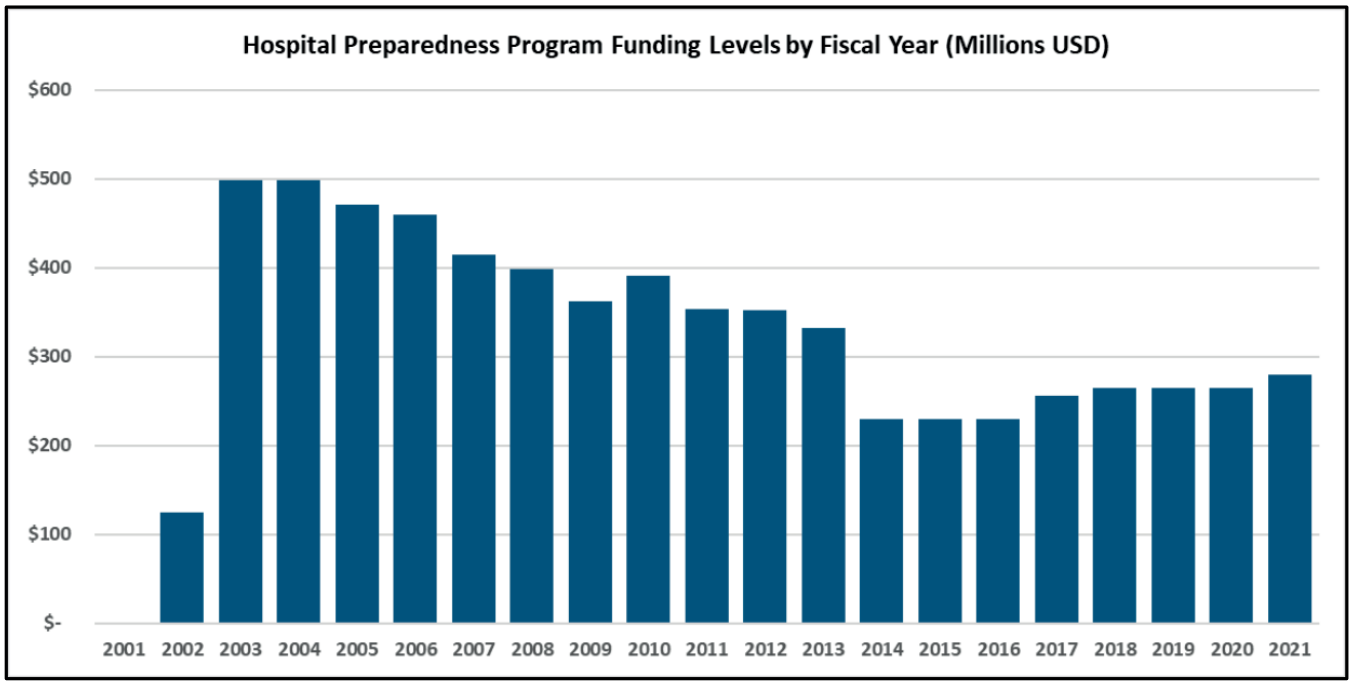


Figure 1 Funding for the US Hospital Preparedness Program (US$m), 2001–2021

Source: Trust for America's Health, 'Hospital Preparedness Program Public Health & Social Services Emergency Fund (PHSSEF) FY 2019 Labor HHS Appropriations Bill', available at: https://www.tfah.org/wp-content/uploads/2018/02/HPP-FY19-request.pdf (accessed 15th April, 2022); Trust for America's Health, 'Hospital Preparedness Program Public Health & Social Services Emergency Fund (PHSSEF) FY 2020 Labor HHS Appropriations Bill', available at: https://www.tfah.org/wp-content/uploads/2019/02/HPP-FY20-request.pd (accessed 15th April, 2022); Trust for America's Health, 'Hospital Preparedness Program Public Health & Social Services Emergency Fund (PHSSEF) FY 2022 Labor HHS Appropriations Bill', available at: https://www.tfah.org/wp-content/uploads/2021/03/FY22_HPP_Fnl.pdf (accessed 15th April, 2022).

response funds do not obviate the need for stability in health and medical preparedness funding, which serves as the foundation on which response actions are surged.[11]

In parallel, cyber attacks on healthcare organisations have been increasing in both frequency and severity. Hospitals and healthcare organisations are increasingly viewed by malicious actors as soft and lucrative targets, with sprawling digital infrastructure, multiple access points and a workflow increasingly reliant on computer systems.[12] When successful, cyber attacks can disrupt and nearly paralyse normal operations, increasing the shock to organisations that already operate under crisis conditions.[13,14] Cyber attacks can be costly not only in terms of damaged hardware and software, but also from the perspective of patient safety, institutional reputation and human resources.[15] Within the healthcare sector, the healthcare workforce — which encompasses a dazzling variety of roles, education levels and technological savvy — has historically shown shockingly low levels of cyber security awareness and practices.[16] Planning for defence and mitigation against cyber attacks in the modern, highly connected healthcare ecosystem, must account for the possibility of accidental or malicious breaches by the very people responsible for the safety and care of patients within it.

This paper considers the intersecting and compounding crises of cyber crime, the COVID-19 pandemic and workforce exhaustion in healthcare. As operating

under crisis conditions becomes the status quo, each new crisis risks catastrophic synergy with the existing crises. The healthcare workforce was stretched thin before the current pandemic; additional vertical crises, such as a system-wide cyber attack, exacerbate effects on an already stressed workforce, leading to decreased efficiency, revenue losses and poorer patient outcomes. Preparatory investment in infrastructure, both human and digital, can blunt these adverse outcomes and increase institutional resilience in the face of future crises.

STRESSORS CONTRIBUTING TO CYBER-SECURITY VULNERABILITIES IN HEALTHCARE

General stressors on healthcare settings

Writing for The Atlantic in November 2021, pre-Omicron wave, Ed Yong described a dedicated but demoralised and depleted workforce seeking relief, in many cases by walking away.[17] Cited in his article are US Bureau of Labor Statistics findings that 500,000 healthcare workers had quit since the pandemic began, along with predictions of more losses, including a report by the American Association of Critical Care Nurses that 66 per cent of critical care and emergency nurses had considered leaving the field of nursing entirely.[18] Outside of hospitals, for example in outpatient and skilled nursing facilities, a decrease of 1.1 million workers was observed from 2019 to 2020, followed by a temporary rebound in 2021.[19] In the American Medical Association's 2020 'Coping with COVID' study, 23.8 per cent of ~9,000 physicians and 40 per cent of ~2,000 nurses planned to exit their practice within two years.[20] In the recently released Elsevier Health 'Clinicians of the Future' report, based on responses by ~3,000 clinicians from 111 countries, 31 per cent of participants overall and 47 per cent of those in the USA said they planned to leave their current job by 2024.[21]

The reasons for healthcare worker attrition are complex but COVID-19 is a clear proximate cause of the current crisis. After two years witnessing the deaths of patients young and old, often despite maximal medical therapy, the work of frontline physicians and clinical staff has become even more tragic and difficult due to the wide circulation of misinformation, vaccine hesitancy and outright pandemic denialism among many patients and their families. The toll of repeat trauma, compassion fatigue and social isolation, has manifested in high rates of depression, anxiety, post-traumatic stress disorder and rising rates of healthcare worker suicides.[22,23] Healthcare jobs are simply more difficult, more dangerous and less rewarding now, even during lulls in COVID-19 transmission, with no time allotted to process and recuperate.[24,25] Before the pandemic, clinicians already faced increasing patient complexity as new technologies enabled patients to live longer even with advanced diseases, albeit with a high level of medical dependence. Since routine medical care was disrupted during the pandemic, patients have been presenting with decompensated and more advanced disease; this too has been exacerbated by decreased in healthcare worker staffing, particularly in primary care.[26]

Healthcare workers will frequently discount risks to themselves to attend to patient safety. However, morale and staffing must be considered patient safety issues. According to ECRI, the top two threats to patient safety are workforce shortages and worker mental health.[27] Indeed, there is a well-established negative correlation between burnout and patient safety, [28] while adequate nursing staffing has been shown to considerably reduce in-hospital mortality.[29] Clearly, this is a dangerous

time for healthcare in the USA. There is an overloaded workforce with high rates of demoralisation and burnout, creating an unsafe environment in which human error is more likely to occur. Given that human error is the most common vector for a successful cyber attack, it is these very conditions that make healthcare organisations particularly enticing targets for cyber criminals.[30,31]

Specific stressors and cyber attack vulnerability

Pandemics historically occur with waves of illness accelerating followed by temporary waning.[32,33] This cycle tends to continue until some sort of herd immunity is reached (through vaccination, prior infection, or a combination of both), or a natural waning of the virus. The pattern from COVID-19 suggests continuing waves, necessitating vigilance against cases and hospitalisations driven by a myriad of factors including, but not limited to, new variant emergence, premature relaxing of protective measures and natural cycles in disease spread.[34,35] Compounding events keep the healthcare system under a state of response, limiting the time and resources available for the sector to prepare for future emergencies, including subsequent pandemic waves and future cyber attacks..

Cyber attacks are not unforeseen, as hospitals have long been considered vulnerable.[36] In 2018, the healthcare sector lost approximately US$3.6bn in revenue to one type of cyber attack, namely business e-mail compromise. Not all costs are reported, but in 2020 UVM reportedly lost US$63m in the space of 40 days.[38] The pandemic has made healthcare more vulnerable due to increasing remote work facilitated by use of remote desktops and VPNs, practices with known security risks.[38]

The incidence of attacks also appears to be growing: in 2021, 963 sites had been affected by August — up from 560 in the whole of 2020.[39] In a review of healthcare cyber security for 2020, the US DHHS Office of Information Security reported significant increases in both ransomware attacks and data breaches of healthcare organisations, noting that 'the COVID-19 pandemic provides criminal opportunities on a scale likely to dwarf anything seen before'.[40] Figure 2 summarises publicly available data on major cyber attacks (defined by the Center for Strategic and International Studies as attacks with US$1m or more in reported losses), as well as a trend towards attacks on larger healthcare companies, demonstrating emboldened threat actors in 2018–2020. As Figure 3 shows, this is against a background of large-scale (defined as costing US$1bn or more) disasters in the country increasing in intensity.

In a Ponemon Institute survey of 597 healthcare organisations, 67 per cent of surveyed organisations reported having experienced a cyber attack, with 33 per cent having experienced more than once.[41] These organisations are losing faith in their ability to handle such attacks: 61 per cent reported poor confidence in defence against attacks. In addition to economic losses, 25 per cent of the organisations surveyed reported an increase in patient mortality. Third-party contracting, which is associated with increased vulnerability, has been on the rise, with an approximately 30 per cent annual increase for tasks such as data storage, management and security; 43 per cent of third-party contractors handle patient health information patient health information, presenting additional targets for hackers.[42]

Vulnerability to cyber crime is not unique to a any one health system, country or hemisphere. In 2017, the UK National Health Service was crippled by a WannaCry ransomware attack that exploited a vulnerability in Windows XP, which was still in

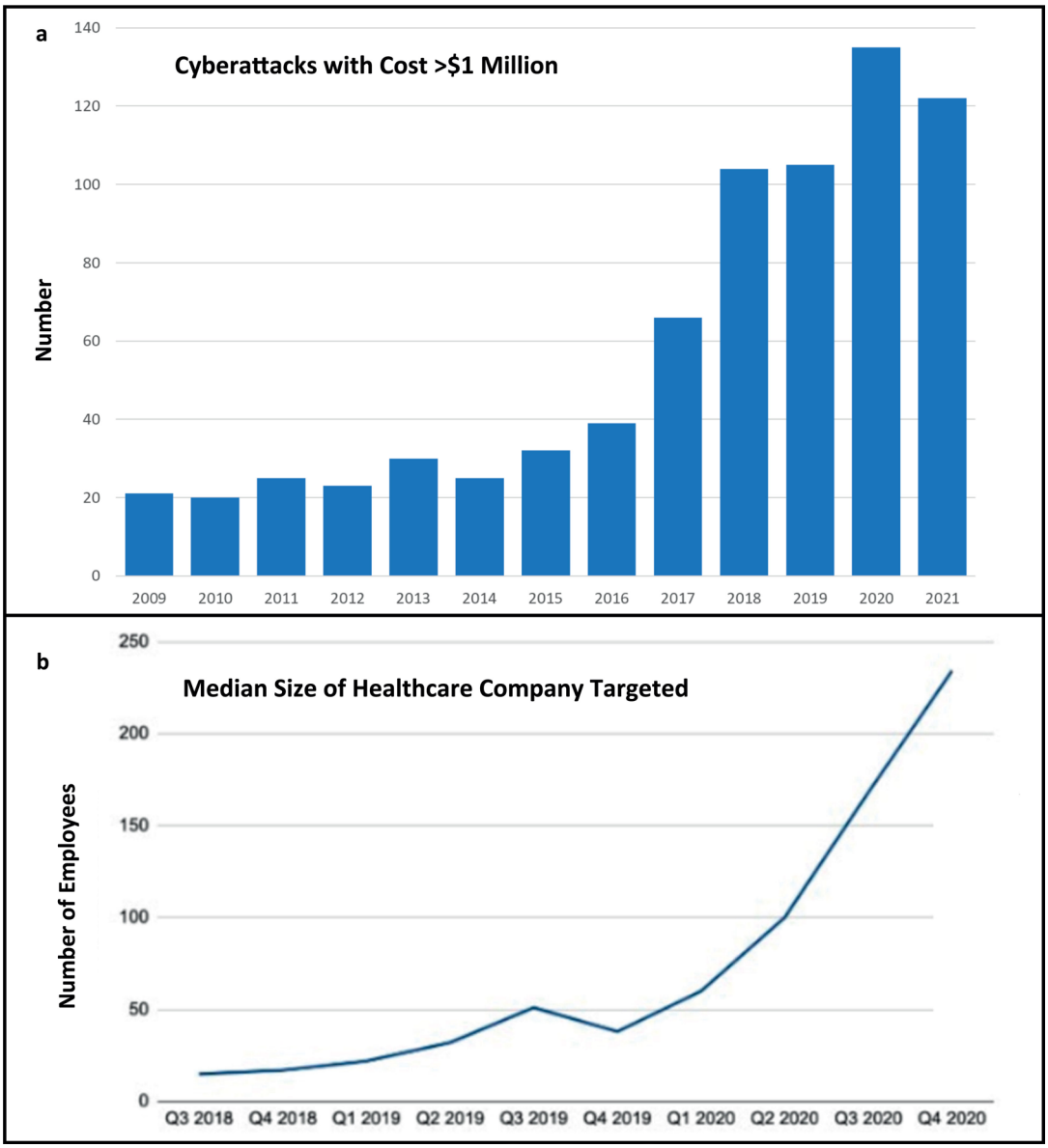


Figure 2 (a) Cyber-attack incidents with US$1 million or more in reported losses, 2009–2021; (b) Trend towards larger-scale ransomware attacks on healthcare companies, 2018–2020

Source: Center for Strategic and International Studies (2022) 'Significant cyber incidents', available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed 24th June, 2022); Goodin, D. (2021) 'Hospitals hamstrung by ransomware are turning away patients', Ars Technica, 16th August, available at: https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/ (accessed 20th March, 2022).

use despite the security patches having expired in 2015. An approximately US$7m deal with Microsoft to continue updating security patches had not been extended due to budgetary reasons; even if the deal had been extended, many NHS facilities were running equipment so outdated they would not have been compatible with the proposed patch. As such, the proposed costs of cyber security maintenance were

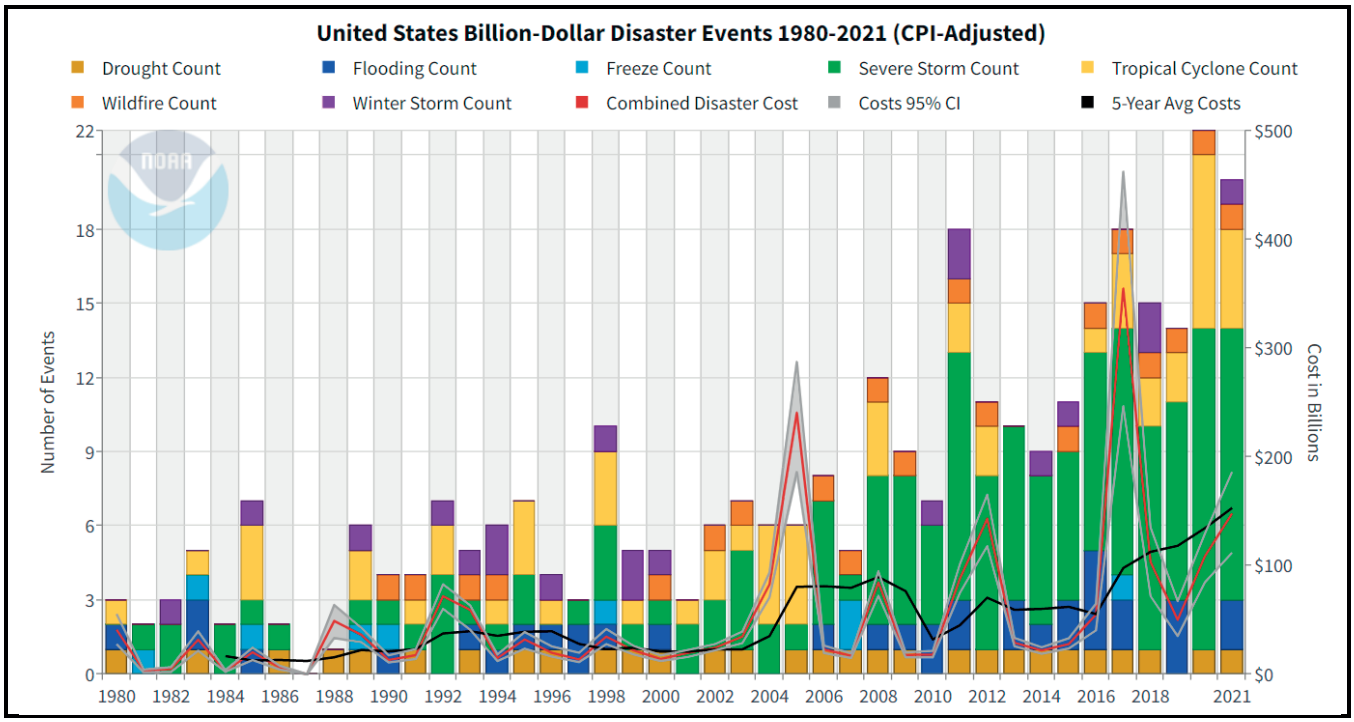


Figure 3 Disaster events with USD 1 billion or more in estimated losses, 1980-2021

Source: US National Oceanic and Atmospheric Administration, National Centers for Environmental Information (2022) 'US billion-dollar weather and climate disasters', available at: https://www.ncei.noaa.gov/access/monitoring/billions/ (accessed 20th March, 2022).

at least US$7m, but that seems a bargain in retrospect; the recovery from WannaCry was estimated to have cost US$4bn.[43,44]

CASE STUDY: CYBER ATTACK ON UHS IN 2020

Event summary and frontline experience

In late September 2020, over 250 Universal Health Services (UHS) hospitals across the USA were affected by a ransomware attack, at that time the largest of its kind, leading to diverted ambulances, cancelled procedures, delayed test results and significant patient safety concerns, not to mention high costs to the system.[45,46] One of the affected facilities was George Washington University Hospital (GWUH), a large academic medical centre in Washington, DC and provider of such functions as level I trauma care, surgical subspecialty care, intensive care (including Extra Corporeal Membrane Oxygenation [ECMO]), the treatment of a large number of COVID-19 patients including their enrolment in clinical trials, and the education of hundreds of medical trainees.

Inpatient services at GWUH were affected for seven days of complete computer downtime (including loss of wireless internet), another 14 days of partial information technology (IT) recovery, and a longer period of downstream effects.[47] Ambulatory services relied on separate electronic medical records (EMR) and IT infrastructure and thus were shielded from direct impact, but indirect effects on shared patients and staff included delayed procedures, degradation in quality of care, resource competition and burnout.[48,49] Medical coding and billing were affected as well, requiring the use of back-up

paper forms during the incident and the additional commitment of staff time afterward, in order to capture charges for the care provided. As the impact of the attack on data ecosystems was harder to quantify, this case study focuses on disruptions to clinical care and the impact on staff, while the next section discusses the risks to data systems along with protective strategies.

Occurring during the upswing of the autumn 2020 wave of COVID-19 in the eastern USA, the cyber attack on UHS further disrupted an already disturbed process. The greatest immediate impact of the EMR outage was on the availability and timeliness of laboratory results and procedural reports as well as other types of clinical documentation. Standard downtime protocols, designed for brief scheduled downtimes, proved inadequate for providing long-term patient care at the existing levels of staffing and patient complexity, leading to potentially unsafe situations requiring further mitigation.[50,51] Risks specific to the care of COVID-19 patients during EMR downtime, identified in the above published accounts as well as in an internal review process by the authors of the present paper included the delayed reporting of SARS-CoV-2 PCR test results, increased risk of inadvertent exposure to COVID-19, difficulty in remotely monitoring unstable patients, increased likelihood of missing drug–drug interactions or errors in written orders for unfamiliar new products, missing windows for enrolment in clinical trials, and the degradation of data available for institutional quality improvement or research activities.

Key elements of the response to the ransomware attack included activation of the emergency operations centre, initial diversion of transfers and postponement of non-emergent procedures, rapid implementation and adjustment of downtime protocols, adoption of multidisciplinary rounding and scheduled check-in practices by inpatient teams, and the promotion of closed-loop communication. These were grounded in existing emergency protocols, an institutional 'culture of safety' approach, and a commitment to restoring routine medical operations as quickly as possible. While some of these mechanisms overlapped with those employed in the response to COVID-19 earlier in the year, other aspects of the response revealed hitherto unknown gaps and areas for innovation. In an assessment of 'lessons learned', leaders of the GWUH medicine residency programme highlighted the 'importance of a hospital-wide, coordinated, multidisciplinary downtime response plan' including special focus on trainee support in areas of documentation, order entry, interdisciplinary communication and centralised information.[52] A separate reflection by the medical faculty group's COVID-19 response lead highlighted the domains of transparent communication by leadership, multi-level stakeholder engagement in safety practices, a culture of 'respectful attention', and structural commitment to resilience with intentional dedication of resources in order to 'move from frontline heroism to sustained survival and recovery'.[53]

Extraordinary efforts by the medical staff, trainees, IT and other support staff at GWUH helped minimise harm and restore clinical operations in the weeks following the ransomware attack. Unfortunately, the timing of the attack and its immediate aftermath consumed the period of time leading into the devastating winter 2020/21 wave of COVID-19. By early November, reported cases in the USA were breaking 100,000 per day for the first time. Although a formal assessment of GWUH clinician morale was not performed at the time, informal feedback from staff and trainees centred on feelings of fatigue and emotional exhaustion from the succession of crises.[54] Morale

received a much-needed boost with the approval and distribution of COVID-19 vaccines starting in December 2020. The work of securing biologic and digital security for the longer term is still ongoing. The overall costs of the incident to UHS were publicly reported as US$67m in lost revenue and recovery costs.[55]

Disruption of data systems

In addition to the immediate disruption to direct patient care and patient safety activities presented above, disruption to an electronic medical record interferes with an institution's ability to store data, recognise patterns, learn from mistakes, optimise performance and perform research. In other words, disruptions in the live environment create failure at the data storage level. For example, whenever a nurse administers medication, it is entered at point of administration in the EMR. Without the EMR, this medication administration is not available for review, cost analysis, resource management, etc. Although the administration record will exist on paper, the review and use of data in this format is cumbersome. More broadly, without an EMR record and timestamps, sentinel events are harder to identify and address, mandatory reporting is more burdensome, and the timing/sequencing of events is more difficult to verify and validate.

It is not uncommon for EMR outages and data systems to be offline for a prolonged period in such an attack. In 2020, a Coveware report found that ransomware causes an average of 15 days of downtime.[56] In a fast-moving crisis such as a pandemic, a lack of live data can be particularly destructive; there are only about two years of data regarding COVID-19, and rapid adjustments have been needed as the virus has swept the globe. GWUH participates in the worldwide collection of real-world data to help guide the global response. The interruption in data collection led to significant gaps in its data; as a result of the UHS cyber attack, relevant information on 30 patients was lost entirely.

More traditional research and clinical trials were also impacted by the cyber attack. Potential study participants, frequently identified by flags in EMR software, could still be enrolled manually by pen and paper, but identifying, educating and enrolling can be a more cumbersome and time-consuming process for an already overworked medical worker, and an unknowable number slipped through the cracks. Important clinical data, such as vital signs and precise medication administration times, can be lost during EMR downtime. Circumstances that affect study participant recruitment, protocol execution and follow-up must be documented; site investigators are responsible for communicating with the study sponsor, the institutional review board and all relevant regulatory entities, to ensure any protocol violations are documented and data integrity is preserved.

To date, healthcare cyber security guidance has focused on the prevention of breaches at the level of individual users, for example, by updating hardware and software, using encryption and two-factor verification technology, instituting 'zero trust' and 'culture of safety' policies, and reducing the number of people with access to sensitive information where possible.[57] Far less information is available on how institutions can best recover once a breach has occurred and what human resources outside of health IT roles are necessary for both prevention and recovery. Based on the guidance published by various institutional, professional and federal entities, general best practices for healthcare cyber security may be summarised as follows:[58–62]

- Implementation of validated cybersecurity measures (eg the National

Institute of Standards and Technology Cybersecurity Framework);
- use of the CIAA principles for cyber security (ie confidentiality, integrity, availability and accountability);
- multiple levels of security controls, including physical (locks), administrative (policies) and technical (encryption);
- use of a series of defensive mechanisms, such that if one were to fail another will take its place;
- frequent, secure backup of data;
- reduction in the number of parties, including external contractors, with access to protected information; and
- continued and targeted cyber security training.

Table 1 outlines how these may be applied to the challenges of a cyber attack on an academic medical centre, stratified by level of impact.

DISCUSSION AND IMPLICATIONS

As with disease, the prevention of cyber attacks is preferable to treatment. Even the most expedient appearing response — capitulation to the hackers' demands — may be ineffective: 80 per cent of small to medium-sized organisations that paid the ransom either did not receive the decryption key or were asked for a second ransom. Further, even rapid capitulation means using a compromised system and time and difficulty returning to previous operations.[63] However, the current models favoured by the healthcare industry do not lend themselves to prevention. The widespread adoption of 'lean' models oriented toward short-term profit and efficient resource use has resulted in a system that is neither secure nor resilient when challenged. Today's reality is one in which healthcare systems face recurrent and compounding crises from pandemic disease and cyber threats. Weathering these challenges and crises requires intervention at the level of funding streams, strategic redundancies and contingencies, along with a culture of support for workforce recovery.[64,65]

On a human level, in the age of COVID-19, all healthcare issues must acknowledge and accommodate the pandemic crisis conditions. Most cyber-security breaches occur due to human error, eg clicking on a phishing e-mail or inappropriately accessing data from an unsecured device or network.[66] Fatigued and disengaged workers are less likely to adhere to cyber-security measures and more likely to fall prey to attacks in spite of routine reminders or modular training.[67] Healthcare worker burnout and cognitive overload are well established as underlying factors contributing to medical error and patient safety violations; best practices by institutions that prioritise safety seek to minimise and mitigate these factors.[68] These factors deserve to be studied formally as root causes contributing to cyber-security vulnerability, and existing planning for health systems security needs to incorporate the perspective of frontline and clinical stakeholders. The present article calls for the concept of information security in the healthcare sector to be reimagined and integrated with greater support for the needs of frontline healthcare workers.

While the above statement is intended to prompt engagement and innovation, it draws on broader patient safety experience. Well-trained, supported, empowered and engaged healthcare workers are key to detecting medical errors and near-misses, and creating an institutional 'culture of safety'.[69] For example, nurses who have in-depth knowledge of facility and patient workflows, may be the first to identify cyber security pain points and issues that others might not see, and should play a key role in institutional planning and response to cyber emergencies.[70]

Table 1: Cyber attack on an academic medical centre — data ecosystem impacts and measures for protection or mitigation

Impact area	*Processes disrupted*	*Protection and mitigation measures*
Direct patient care; emergency medical records	Admission/transfer orders Vital signs monitoring Isolation status Medication orders Laboratory results Pathology reports Imaging/radiology reports Clinician notes Procedure reports and findings Case management and care coordination notes Medical coding and billing	Culture of safety Downtime protocols and training Downtime charts, paper prescriptions, order forms, etc. Centralised communication boards Scheduled and *ad hoc* in-person communication with laboratory, radiology and other departments Multidisciplinary rounding Closed-loop communication of key findings and orders Support from additional staff (eg clinical pharmacists) Additional training for less-experienced care team members Decompression of facility and staff (eg diversion of ambulances, postponement of non-emergent procedures)
Data collection systems	Timed uploads from 'live' EMR environment to data storage Data availability for current and future retrieval/review	EMR-specific cyber-security measures Scanning of paper records for long-term storage Investigating use of standardised forms
Real-world data research	Data on disease characteristics Data on efficacy of interventions Data on time-sensitive diseases (eg dominant COVID-19 variants or seasonal influenza strains)	Database creation for patients who were cared for during the outage Use of retrospective data entry from paper records
Clinical trials	Identification of eligible patients based on 'live' EMR information Timely enrolment in clinical trials Timely initiation of investigational drug or intervention Data collection on enrolled patients	Communication between study staff, investigators and sponsor Communication between study staff and clinical teams Study eligibility 'pocket cards' Manual collection and entry of data by study staff
Patient safety & quality improvement	Deciphering handwritten documentation Omission or miscommunication in verbal orders or reports Detection of errors in prescribing Drug–drug interaction checking Reporting and review of sentinel events Timely reporting to regulatory bodies	Culture of safety Downtime protocols and training Manual review of charts Peer review of orders Closed-loop communication Support from additional staff Additional training geared to specific team-member needs Communication between healthcare leaders and regulatory bodies

The pandemic has taken a particularly brutal toll on nurses, with unprecedented rates of burnout, turnover, retirement and disability.[71] Institutions must therefore be prepared to make investments and structural changes in order to retain experienced skilled personnel. Highly specialised healthcare workers like doctors and nurses can be assisted and empowered with support by those less specialised, eg employing medical scribes has been shown to reduce staff burnout.[72] In a similar vein, ensuring adequate staffing for healthcare-related tasks not requiring nursing or medical degrees, eg clerical, patient transporters, etc., can help offload work from overburdened highly credentialed workers requiring more extensive training. Preserving precious workforce means ensuring adequate recovery time and space for decompression after stressful or traumatic events. The US ASPR TRACIE, in discussion of the incident command structure on COVID-19 response, recommends encouraging paid time off or vacation time during 'troughs' in viral transmission to aid in recovery.[73]

Health IT specialists deserve recognition as another type of healthcare worker, and extending to them the same support given to patient-facing staff can improve resilience and improved response to digital challenges. Most cyber-security breaches are due to human error — a thoughtless click on an e-mail attachment can bring an entire health system to its knees. As such, integrating human and digital resilience is essential. Increased workload leads to a statistically significant increase in likelihood to click on a phishing e-mail link.[74] Further, healthcare workers are not experts in information technology and security, and may not understand the importance of, for example, using IT approved devices as opposed to personal devices. Improved awareness of cyber threats can help align the various healthcare stakeholders in maintaining cyber security[75] but must not come at the expense of exacerbating fatigue or burnout.[76]

On the digital level, investment in digital infrastructure is paramount to ensure that vulnerabilities in hardware and software are addressed, and have the necessary security, redundancy and contingency to survive the unexpected. Healthcare organisations frequently lag other large companies dealing with sensitive data, such as financial institutions and Fortune 1000 firms, on security ratings. Adopting best practices of such firms can provide benchmarks for improvement.[77] However, there are unique challenges to managing healthcare data, and outsourcing cyber security to third-party firms is common, given that the expertise of healthcare organisations lies elsewhere. This has its own risks, including increasing the points via which malicious actors may gain access to a system, but allows scarce resources to be otherwise expended. [78] Ultimately, a reasonable goal of healthcare IT security to decrease end-point complexity: more varieties of devices and programs accessing the central system leads to more points of vulnerability. Reducing this complexity and variety streamlines security measures. When integrating systems, such as telehealth systems, the fewer unsecured devices and programmes with access to the broader system, the fewer points of access for hackers. Implementing such measures requires alignment among the many stakeholders with various goals and understanding of cyber security. A hospital has many teams, among them, information security, information technology, administration, medical staff, materials management and others. Increased coordination regarding security measures, why they are implemented and best practices for maintenance, reduces risk.[79]

The preceding case study of the cyber attack on UHS at GWUH incorporates

two prior reports — respectively emphasising the experiential[80] and operational[81] aspects of the event — in rough parallel with the human and digital domains in this discussion. The 'lessons learned' emphasise the importance of institutional culture, interdisciplinary collaboration, investment in human and technological infrastructure and giving special attention to the needs of trainees in the healthcare professions. A report from another US healthcare institution affected by the same attack likewise notes the importance of institutional memory and the key role of non-physician healthcare workers — in that case, critical care pharmacists integrated into an ICU team — in maintaining patient safety during the crisis.[82] Another key aspect of the present case is the identity of GWUH as a teaching institution. Medical trainees are some of the least experienced, most vulnerable to burnout, but also most flexible and innovative stakeholders in the system, and should be routinely included in institutional planning for safety and resilience. Potential educational interventions to improve cyber-security preparedness (in addition to now-standard individual training modules) include team-based exercises or simulation trainings featuring cyber attack or downtime situations.[83] More broadly, an institutional 'culture of safety' approach to cyber security would incorporate beliefs, attitudes and actions across all levels as a bulwark against other threats to patient safety. Figure 4 summarises some of the common mechanisms of vulnerability and protective factors shared by pandemic, cyber and workforce-related threats to healthcare.

At the national level, more consistent and substantial support of the healthcare sector for preparedness is necessary to build resilience for a wide range of threats. The long-term impacts from the COVID-19 pandemic are not yet fully known, but certainly there will be degradation of readiness from non-stop pandemic response, in addition to cyber attacks and other stressors

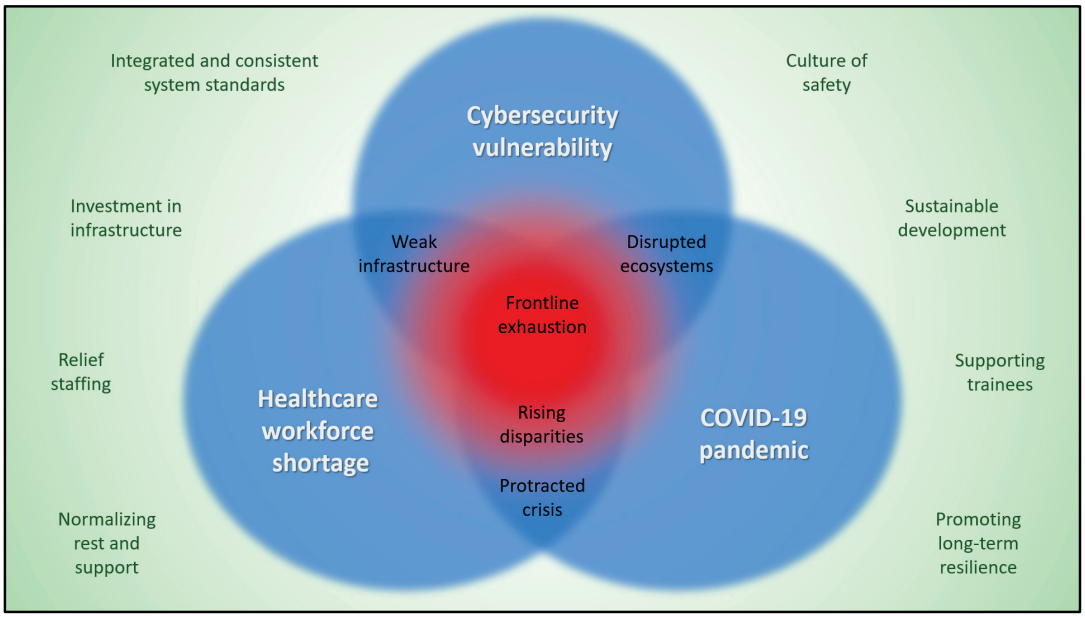


Figure 4 Common vulnerabilities and protective factors in pandemic, cyber and workforce shortage crises in healthcare

on healthcare systems. Investments in preparedness and resilience should be made at all levels, including at the national level as health is an important component of national security and is on the frontlines of homeland defence. While successive and compounding crises threaten to deplete the national healthcare workforce, large-scale investment in restorative and safety-focused interventions in this sector would present an opportunity to recover from a generational crisis and to pre-emptively strengthen vulnerable systems ahead of the next crisis.

Ultimately, the above recommendations seek to proactively prepare for the next crisis at the same time as confronting those already here. COVID-19, staffing shortages and data vulnerabilities are all part of the healthcare landscape. None of these crises have a foreseeable endpoint at this time, and so must be addressed in the long term. To manage these crises and those yet to manifest, infrastructure and funding streams must shift away from short-term/reactive approaches to compounding crises, including the ones discussed in this paper, in favour of building workforce and infrastructure for resilience. Crises need not be disasters and they need not be catastrophes, but absent forethought and planning, the only response to a crisis is short-term, reactive survival mode. As the short term stretches into the long, survival mode becomes less and less sustainable, and unless addressed, it becomes a crisis of its own.

CONCLUSION

Medicine is a hard job worth doing well, and the regular challenges of its practice have been exacerbated by trends towards staffing shortages and the unique difficulties of the COVID-19 pandemic. Cyber attacks on healthcare organisations were increasing pre-pandemic and have increased again during it, exploiting digital and human vulnerabilities. Economic trends and policies in healthcare have shaped the confounding reality of healthcare worker burnout, 'lean' staffing and the increased complexity of medical care, creating a field rife with risk and short on the redundancies that provide for a more resilient response. The sprawling digital health infrastructure and overburdened healthcare workforce have proven themselves vulnerable to cyber criminals, with painful impacts on patient care and safety, as well as on institutional finances and reputations. It is imperative that healthcare institutions begin to reverse these trends, not merely by creating cyber security plans and contingencies, but by centring the needs of healthcare workers in this planning. Ultimately, preparing for future crises is safer and more sustainable than reacting to current, cascading crises, and investing in human capital pays dividends in resilience for the future.

REFERENCES

(1) American Hospital Association (2018) 'Trendswatch Chartbook: Trends Affecting Hospitals and Systems', available at: https://www.aha.org/system/files/2018-07/2018-aha-chartbook.pdf (accessed 24th June, 2022).

(2) Healthcare Cost and Utilization Project (April 2021) 'HCUP Fast Stats: Trends in Emergency Department Visits', Agency for Healthcare Research and Quality, Rockville, MD', available at: www.hcup-us.ahrq.gov/faststats/national/inpatienttrendsED.jsp (accessed 24th June, 2022).

(3) Kelen, G. D., Wolfe, R., D'Onofrio, G., Mills, A. M., Diercks, D., Stern, S. A., Wadman, M. C. and Sokolove, P. E. (September 2021) 'Emergency department crowding: the canary in the health care system', *New England Journal of Medicine*, Vol. 2, No. 9,

available at: https://catalyst.nejm.org/doi/full/10.1056/CAT.21.0217 (accessed 24th June, 2022).
(4) US Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation (2021) 'Trends in the Utilization of Emergency Department Services, 2009–2018', available at: https://aspe.hhs.gov/pdf-report/utilization-emergency-department-services (accessed 24th June, 2022).
(5) Buerhaus, P. I., Auerbach, D. I. and Staiger, D. O. (May 2017) 'How should we prepare for the wave of retiring baby boomer nurses?' *Health Affairs Blog*.
(6) Boyle, P. (September 2020) 'Medical school enrollments grow, but residency slots haven't kept pace', *Association of American Medical Colleges*, 3rd September, available at: https://www.aamc.org/news-insights/medical-school-enrollments-grow-residency-slots-haven-t-kept-pace (accessed 20th March, 2022).
(7) Institute of Medicine (2009) 'Ensuring Quality Cancer Care Through the Oncology Workforce: Sustaining Care in the 21st Century: Workshop Summary', The National Academies Press, Washington, DC.
(8) Trust for America's Health (2018) 'Hospital Preparedness Program Public Health & Social Services Emergency Fund (PHSSEF) FY 2019 Labor HHS Appropriations Bill', available at: https://www.tfah.org/wp-content/uploads/2018/02/HPP-FY19-request.pdf (accessed 15th April, 2022).
(9) Trust for America's Health (2019) 'Hospital Preparedness Program Public Health & Social Services Emergency Fund (PHSSEF) FY 2020 Labor HHS Appropriations Bill', available at: https://www.tfah.org/wp-content/uploads/2019/02/HPP-FY20-request.pd (accessed 15th April, 2022).
(10) Trust for America's Health (2021) 'Hospital Preparedness Program Public Health & Social Services Emergency Fund (PHSSEF) FY 2022 Labor HHS Appropriations Bill', available at: https://www.tfah.org/wp-content/uploads/2021/03/FY22_HPP_Fnl.pdf (accessed 15th April, 2022).
(11) Schlegelmilch, J., Petkova, E. and Redlener, I. (2015) 'Disaster prepared: How federal funding in the USA supports health system and public health readiness', *Journal of Business Continuity & Emergency Planning*, Vol. 9, No. 2, pp. 112–118.
(12) Zetter, K. (March 2016) 'Why hospitals are the perfect targets for ransomware', *Wired*, available at: http://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets (accessed 20th March, 2022).
(13) Clarke, R. and Youngstein, T. (2017) 'Cyberattack on Britain's National Health Service — a wake-up call for modern medicine', *New England Journal of Medicine*, Vol. 377, No. 5, pp. 409–411.
(14) Akselrod, H. (2021) 'Crisis standards of care: Cyber attack during a pandemic', *Annals of Internal Medicine*, Vol. 174, No. 5, pp. 713–714.
(15) Hood, C. (2021) 'Telehealth cybersecurity', in Sikka, N. (ed.), *A Practical Guide to Emergency Telehealth*, Oxford University Press, New York, NY, pp. 81–92.
(16) Landi, H. (August 2019) 'Survey finds alarming number of healthcare workers have not had cybersecurity training', *Fierce Healthcare*, available at: https://www.fiercehealthcare.com/tech/despite-ongoing-cyber-threats-32-healthcare-employees-never-received-cybersecurity-training (accessed 24th June, 2022).
(17) Yong, E. (November 2021) 'Why healthcare workers are quitting in droves', *The Atlantic*, available at: https://www.theatlantic.com/health/archive/2021/11/the-mass-exodus-of-americas-healthcare-workers/620713/ (accessed 20th March, 2022).
(18) *Ibid*.
(19) Cantor, J., Whaley, C., Simon, K. and Nguyen, T. (2022) 'US health care

workforce changes during the first and second years of the COVID-19 pandemic', *Journal of the American Medical Association Health Forum*, Vol. 3, No. 2.
(20) Abbasi, J. (2022) 'Pushed to their limits, 1 in 5 physicians intends to leave practice', *Journal of the American Medical Association*, Vol. 327, No. 15, pp. 1435–1437.
(21) Elsevier Health (March 2022) 'Clinician of the Future: A 2022 Report', available at: https://www.elsevier.com/connect/clinician-of-the-future (accessed 21st March, 2022).
(22) Joseph, A. (March 2022) '"I fear the long-term effects": Before his death, a nurse warned of the pandemic's toll on health care workers', *STAT News*, available at: https://www.statnews.com/2022/03/23/nurse-warned-of-pandemic-mental-toll-health-workers/ (accessed 23rd March, 2022).
(23) Abbasi, ref. 20 above.
(24) Ibid.
(25) Hollingsworth, H. and Schulte, G. (September 2021) 'Health workers once saluted as heroes now get threats', AP News, available at: https://apnews.com/article/coronavirus-pandemic-business-health-missouri-omaha-b73e167eba4987cab9e58fdc92ce0b72 (accessed 20th March, 2022).
(26) Wells, K. (October 2021) 'ERs are now swamped with seriously ill patients — but many don't even have COVID', National Public Radio, available at: https://www.npr.org/sections/health-shots/2021/10/26/1046432435/ers-are-now-swamped-with-seriously-ill-patients-but-most-dont-even-have-covid (accessed 23rd March, 2022).
(27) Cheney, C. (March 2022) 'Workforce shortages identified as top patient safety concern of 2022', *Health Leaders*, available at: https://www.healthleadersmedia.com/clinical-care/workforce-shortages-identified-top-patient-safety-concern-2022 (accessed 23rd March, 2022).
(28) Garcia, C. L., Abreu, L. C., Ramos, J. L. S., Castro, C. F. D., Smiderle, F. R. N., Santos, J. A. D. and Bezerra, I. M. P. (2019) 'Influence of burnout on patient safety: Systematic review and meta-analysis', *Medicina (Kaunas)*, Vol. 55, No. 9.
(29) Driscoll, A., Grant, M. J., Carroll, D., Dalton, S., Deaton, C., Jones, I., Lehwaldt, D., McKee, G., Munyombwe, T. and Astin, F. (2018) 'The effect of nurse-to-patient ratios on nurse-sensitive patient outcomes in acute specialist units: A systematic review and meta-analysis', *European Journal of Cardiovascular Nursing*, Vol. 17, No. 1, pp. 6–22.
(30) He, Y., Aliyu, A., Evans, M. and Luo, C. (2021) 'Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review', *Journal of Medical Internet Research*, Vol. 23, No. 4, e21747; erratum in *Journal of Medical Internet Research*, Vol. 23, No. 4, e29877.
(31) Jalali, M. S. and Kaiser, J. P. (2018) 'Cybersecurity in hospitals: A systematic, organizational perspective', *Journal of Medical Internet Research*, Vol. 20, No. 5.
(32) United States Centers for Disease Control and Prevention (US CDC) (2016) 'Pandemic Intervals Framework', available at: https://www.cdc.gov/flu/pandemic-resources/national-strategy/intervals-framework.html (accessed March 22, 2022).
(33) Cacciapaglia, G., Cot, C. and Sannino, F. (2021) 'Multiwave pandemic dynamics explained: How to tame the next wave of infectious diseases', *Scientific Reports*, Vol. 11, No. 1.
(34) *Ibid*.
(35) Johns Hopkins University Coronavirus Resource Center (2022) 'United States', available at: https://coronavirus.jhu.edu/region/united-states (accessed 23rd March, 2022).
(36) Zetter, ref. 12 above.
(37) Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C. and Tariverdi, M. (2021) 'Assessing resilience of hospitals to cyberattack', *Digital Health*, Vol. 7.
(38) He *et al.*, ref. 30 above.

(39) Goodin, D. (August 2021) 'Hospitals hamstrung by ransomware are turning away patients', *Ars Technica*, available at: https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/ (accessed 20th March, 2022).
(40) US Department of Health and Human Services Office for Information Security (2020) 'A retrospective look at healthcare cybersecurity', available at: https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf (accessed 10th April, 2022).
(41) Ponemon Institute (2022) 'The impact of ransomware on healthcare during COVID-19 and beyond', *Ponemon Research Report*, available at: https://www.censinet.com/ponemon-report-covid-impact-ransomware/ (accessed 20th March, 2022).
(42) *Ibid*.
(43) Berr, J. (May 2017) '"WannaCry" ransomware attack losses could reach $4 billion', CBS News, available at: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ (accessed 15th March, 2022).
(44) Clarke and Youngstein, ref. 13 above.
(45) Akselrod, ref. 14 above.
(46) Davis, J. (March 2021) 'UHS ransomware attack cost $67m in lost revenue, recovery efforts', *Health IT Security*, available at: https://healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue (accessed 23rd March, 2022).
(47) Paul, C., Bilger, E., Kango, G., Reyes, J. A. and Catalanotti, J. S. (2021) 'Residency program preparedness for prolonged downtime: Lessons learned from a cyberattack', *Journal of Graduate Medical Education*, Vol. 13, No. 5, pp. 626–630.
(48) *Ibid*.
(49) Akselrod, ref. 14 above.
(50) *Ibid*.
(51) Paul *et al*., ref. 47 above.
(52) *Ibid*.
(53) Akselrod, ref. 14 above.
(54) *Ibid*.
(55) Davis, ref. 46 above.
(56) US DHHS OIS, ref. 40 above.
(57) Hood, ref. 15 above.
(58) *Ibid*.
(59) US DHHS OIS, ref. 40 above.
(60) McGuiness, T. (2001) 'Defense in depth', available at: http://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525 (accessed 28th August, 2014).
(61) Murphy, S. P. (2018) 'Impact of information privacy and security on health IT', in *Healthcare Information Security and Privacy*, McGraw Hill, New York, NY, pp. 225–254.
(62) US National Institute of Standards and Technology (US NIST) (2018) 'Cybersecurity Framework Version 1.1', available at: https://www.nist.gov/cyberframework (accessed 11th April, 2022).
(63) Ghayoomi *et al*., ref. 37 above.
(64) Akselrod, ref. 13 above.
(65) Schlegelmilch J. (2020) *Rethinking Readiness: A Brief Guide to Twenty-First-Century Megadisasters*, Columbia University Press, New York, NY.
(66) He *et al*., ref. 30 above.
(67) Reeves, A., Delfabbro, P. and Calic, D. (2021) 'Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue', *SAGE Open*, Vol. 11, No. 1, pp. 1–18.
(68) ECRI (June 2019) 'Culture of safety: An overview', *Health System Risk Management*, available at: https://www.ecri.org/components/HRC/Pages/RiskQual21.aspx (accessed 5th April, 2022).
(69) *Ibid*.
(70) Eddy, N. (May 2022) 'Nurses are vital to maintaining healthcare cybersecurity', *HealthTech*, available at: https://healthtechmagazine.net/article/2022/05/nurses-are-vital-maintaining-healthcare-cybersecurity (accessed 24th June, 2022).

(71) Yong, ref. 17 above.
(72) Driscoll *et al.*, ref. 29 above.
(73) Alberts, E., Aronson, S., Bennett, M. E., DeAtley, C., Hick, J. and Puentes, L. (2021) 'The effect of COVID-19 on the healthcare incident command system', ASPR TRACIE', available at: https://files.asprtracie.hhs.gov/documents/aspr-tracie-the-effect-of-covid-19-on-the-healthcare-ics.pdf (accessed 20th March, 2022).
(74) He *et al.*, ref. 30 above.
(75) Jalali and Kaiser, ref. 31 above.
(76) Reeves *et al.*, ref. 67 above.
(77) Choi, S. J. and Johnson, M. E. (2021) 'The relationship between cybersecurity ratings and the risk of hospital data breaches', *Journal of the American Medical Informatics Association*, Vol. 28, No. 10, pp. 2085–2092.
(78) Schlegelmilch, ref. 65 above.
(79) Jalali and Kaiser, ref. 31 above.
(80) Akselrod, ref. 14 above.
(81) Paul, ref. 47 above.
(82) Haase, K. K., Whitworth, M. M. and Yalamanchili, K. (2021) 'Clinicians' experiences and reflections from a health system cyberattack', *Journal of the American College of Clinical Pharmacy*, Vol. 4, No. 6, pp. 738–742.
(83) Willing, M., Dresen, C., Gerlitz, E., Haering, M., Smith, M., Binnewies, C., Guess, T., Haverkamp, U. and Schinzel, S. (2021) 'Behavioral responses to a cyber attack in a hospital environment', *Scientific Reports*, Vol. 11, No. 1.