University of Colorado Law Review

Volume 90 | Issue 1 Article 7

Winter 2019

Who Guards the Guardians? Simplifying the Discovery of Electronic Medical Records

Joseph DeAngelis

WHO GUARDS THE GUARDIANS? SIMPLIFYING THE DISCOVERY OF ELECTRONIC MEDICAL RECORDS

Joseph DeAngelis*

As medical errors reign as a leading cause of death and injury in the United States, the efficient and effective resolution of medical negligence disputes becomes increasingly necessary, albeit uncommon. Despite the frequency of medical errors, the quality of medical care in the United States has increased over the last several decades. This improvement has been due in no small part to the widespread adoption of Electronic Medical Records (EMRs) by healthcare providers across the country. While EMR systems have done their part to improve patient care, they are not designed for litigation. Indeed, the widespread use of EMR technology has created several unresolved legal issues that unnecessarily complicate the discovery process in medical negligence litigation.

The substantial confusion surrounding the discovery of information within EMR systems invariably leads to an unnecessary motions practice that overburdens the judicial system's limited resources. Three common and related legal problems include the "Privilege Problem," the "Production Problem," and the "Preservation Problem." The Privilege Problem concerns the possible interplay between HIPAA and the rules of discovery. The Production Problem refers to the undue costs and unreliability of a reproduced medical record

---

* J.D. Candidate, 2019, University of Colorado Law School; Casenote and Comment Editor, *University of Colorado Law Review*. Thanks to everyone who supported this project. In particular, I would like to thank my editors, Timbre Shriver, Marty Whalen Brown, Claire Jarrell, and Rob McCary, for all their help throughout this project. I would also like to thank Professors John Francis and Matthew Weber for allowing me to bounce ideas off of them in the early stages of this project. This project would certainly have suffered without their insight. I would also like to thank my mother for giving me the idea to write this in the first place. Listening to you vent your frustrations definitely helped me develop this Comment. And to Autumn, thank you for your patience and support during the endless nights writing and revising and revising and revising. I couldn't have done this without you.

for purposes of litigation. The Preservation Problem arises from the need to regularly update patient information. This Comment recommends that all litigants in a medical negligence action should have remote access to a patient's EMR file and that certain changes should be made to the design of EMRs to ensure the integrity and reliability of the record during litigation.

INTRODUCTION

Medical errors are currently the third leading cause of death in the United States, surpassed only by heart disease and cancer.[1] That figure becomes even more frightening considering that it only counts deaths but does not account for other debilitating injuries resulting from medical errors.[2] Studies estimate that between one-eighth and one-third of all patients will suffer some injury caused by medical management rather than their underlying injury.[3] Of these injuries, more than one-quarter are due to negligence.[4] When a patient or her family believes that the cause of the injury is medical negligence, they may file a lawsuit against the provider to recover damages.

As the official documentation of care, medical records are indispensable in any lawsuit for medical negligence.[5] Discovery of medical records that are stored in an electronic format, however, is often contentious, time-consuming, and expensive.

Before medical providers digitized their records, discovery of medical records was relatively straightforward because medical records existed exclusively on paper. When a patient requested her own records, a "copy" would be produced by way of a photocopier. Any changes and notes were easily identifiable from strike-throughs, and discovery was simple. As healthcare delivery advanced, so too did the manner of documenting care. Large-scale healthcare operations with a variety of specialists required an easier way to document and share the details of patient care. The problem of illegible handwriting needed to be solved. The necessity of timely care required that

---

1. Martin A. Makary & Michael Daniel, *Medical Error—the Third Leading Cause of Death*, BMJ (2016), https://www.bmj.com/content/353/bmj.i2139 [https://perma.cc/LK8F-QHJG] (estimating the number of deaths from medical errors based on a meta-analysis of data taken from other studies).

2. *See id.* (discussing only the number of deaths).

3. BARRY R. FURROW ET AL., HEALTH LAW: CASES, MATERIALS AND PROBLEMS 42–43 (7th ed. 2013).

4. *Id.* at 40.

5. *Id.* at 261–62.

accurate and up-to-date information be available to caregivers. To meet these demands, changes needed to be made.

The solution has been the widespread, federally subsidized adoption of electronic medical records, or EMRs.[6] In most respects, an EMR is simply an electronic version of the paper medical record. Because they exist in a digitized format, however, EMRs have the added functionality of facilitating communication among providers, capturing billing information, alerting staff to changing conditions, and automatically updating the record to reflect the patient's current condition.[7] To encourage these beneficial features of EMRs, federal and state governments have heavily subsidized the universal adoption of EMRs in hospitals.[8] Specifically, the Affordable Care Act subsidizes a hospital's use of EMRs under Medicare and Medicaid if the hospital's EMR system meets Medicare's "meaningful use requirements," such as the ability to communicate with other EMR systems, the ability to maintain an active medication list, and the ability to list current and active diagnoses.[9] As a result of these subsidies, EMRs are now the standard method of documenting patient care.

While EMRs have certainly played their role in improving the effective and efficient delivery of healthcare, interpreting printouts of EMRs can be a nightmare for lawyers. For a variety of reasons discussed in this Comment, EMRs look very different on paper or in PDF format than they do on a doctor's or a nurse's screen. Consequently, a lawyer spends an

---

6. This Comment refers to electronic medical records (EMRs) and electronic health records (EHRs) collectively as EMRs. While the two systems are different, this Comment refers to them collectively for the sake of brevity. An EMR is a localized medical record, or the electronic version of a patient's chart. An EHR is broader, compiling a patient's EMRs from various providers into one digital corpus and incorporating patient history, etc. *See* Peter Garrett & Joshua Seidman, *EMR vs EHR*, HEALTHIT (Jan. 4, 2011), https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/ [https://perma.cc/2VGW-JH35]. Because both contain information relevant to a patient's care, and because both should be provided in the designated record set (discussed in Part III, *infra*), referring to them collectively for the purposes of discovery is appropriate.

7. *See infra* Part I (discussing the purpose and functions of EMRs).

8. *See generally Meaningful Use Glossary and Requirements Table*, AM. MED. ASS'N, http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/Code49_%20AMA%20Meaningful%20use%20glossary%20and%20requirements-table.pdf (last visited Mar. 16, 2018) [https://perma.cc/98JK-WXGA] (listing the meaningful use requirements).

9. *See id.*

unnecessary amount of time during discovery interpreting and authenticating the record.[10] Despite this current reality, EMRs theoretically have the potential to facilitate streamlined and effective dispute resolution, holding certain healthcare providers accountable for mistakes while shielding others from illegitimate claims. However, until EMR systems provide a readable, usable, and exportable means for adverse parties to inspect the record, EMR discovery will continue to delay the resolution of medical negligence litigation, driving up its cost to the detriment of all parties.

This Comment argues that while the rules of discovery provide an adequate theoretical basis upon which to streamline EMR discovery, current solutions fail to live up to the intended spirit of discovery. Of course, several background assumptions guide this analysis. Most importantly, the spirit of discovery is one that balances fairness and limitations. Discovery should strive for equitable access to material information.[11] The proper scope of discovery must encompass enough information to ensure that neither party is concealing facts and to prevent surprise at trial, but the scope cannot be so broad as to harass or unduly burden the producing party.[12] For several reasons detailed throughout this comment, EMR discovery often fails to satisfy this ideal.

Another background assumption is that healthcare providers[13] tend to have their patients' best interests in mind and genuinely try to provide the best care possible. Providers, however, are also human and can be tempted to cover up mistakes if given the opportunity. Although courts should never presume malice or deceit, adequate safeguards should be in place to check shortcomings in human nature.

The final background assumption is that patients and providers all benefit from efficient and cost-effective dispute resolution in which both parties possess reliable information. Patients specifically benefit from access to a forum that permits them to recover just compensation for a legitimate injury.

---

10. *See infra* Part III (discussing the Production Problem).

11. This sentence, and the one preceding it, represent the author's personal philosophy on discovery. The reasons that I feel this assumption is a fair one are more fully articulated in Section III.E (discussing the policy reasons informing the scope of discovery).

12. *See* Hickman v. Taylor, 329 U.S. 495, 507–08 (1947).

13. Throughout this Comment, "providers" refers generally to hospitals, doctors, physician's assistants, and nurses, unless otherwise specified.

And of course, patients and providers alike benefit from streamlined discovery that requires fewer experts, fewer re-depositions, and a shorter duration of discovery. Physicians, nurses, and other mid-level providers also enjoy some unique benefits from streamlined discovery. Most physicians face lawsuits during their career, but the vast majority of these lawsuits are mitigated or dropped after a careful review by medical negligence attorneys with access to a reliable medical record.[14] In fact, only 6 percent of doctors pay claims for medical negligence because of a settlement or adverse judgment.[15] An accurate and authenticated record enables providers to better filter legitimate and defensible claims, and to better determine which claims should be settled, which could be defended at trial, and which could proceed to summary judgment. An efficient discovery process with reliable and discernable medical records thus helps litigants quickly determine the merits of medical negligence claims, expediting litigation and removing a significant source of stress for practicing physicians.

Hospitals—and especially doctors—should demand that EMR technologies be designed to allow access by other users in a format that provides an accurate and reliable record of the care provided to their patients when disputes regarding patient care arise. The appropriate solution, however, must be found not only by considering the rules of discovery and the costs of litigation but also by looking to the privacy and quality concerns that lie at the heart of healthcare delivery.

This Comment begins in Part I by comparing and contrasting the overarching objectives of healthcare delivery and dispute resolution, concluding that EMRs can provide a platform that reconciles those competing interests. The "Privilege Problem" and "Production Problem" discussed in Parts II and III, respectively, show that the confusion surrounding the authorities governing medical records' discoverability creates unnecessary discovery disputes that clog up the courts with discovery motions. The discussion about the Production

---

14. *See* Emily Walker, *Most Doctors Will Face Malpractice Suit, AMA Says*, ABC NEWS (Aug. 5, 2010), http://abcnews.go.com/Health/HealthCare/malpractice-lawsuits-doctors-common-ama/story?id=11332146 [https://perma.cc/B6C2-6XBR] (finding that most claims against doctors are not paid out).

15. Anna Almendrala, *Many Doctors Who Face Malpractice Suits Are Serial Offenders*, HUFFINGTON POST (Jan. 29, 2016), https://www.huffingtonpost.com/entry/doctors-malpractice-research_us_56a94bece4b05e4e37033d00 [https://perma.cc/RPG6-VRUF].

Problem also touches on the ways in which a confusing, incomplete record increases discovery costs and fails to comply with the proportionality factors espoused by the 2015 amendments to the Federal Rules of Civil Procedure (FRCP). Finally, in its discussion of the "Preservation Problem," Part IV describes how, without some adequate preservation function, the mutability of the record hinders plaintiffs seeking legitimate compensation, exposes defendants to potential liability, and hurts both parties' credibility at trial. This Comment ultimately concludes that Congress and the Centers for Medicare and Medicaid Services (CMS) should update the EMR's meaningful use requirements by encouraging EMR designs that facilitate efficient and effective dispute resolution consistent with the spirit of discovery.[16] But in the event that Congress and CMS do not update the meaningful use requirements, this Comment proposes several other solutions available to courts.

I. THE DUELING PURPOSES OF PATIENT CARE AND MEDICAL NEGLIGENCE LITIGATION

Any meaningful analysis of the problems that EMRs pose to litigation and dispute resolution must be framed according to the interests at stake. EMRs serve different needs when used by healthcare providers than when used in dispute resolution. Because healthcare providers are ultimately the consumers of EMR technologies, however, EMRs are designed for the needs of healthcare providers. To illustrate how market forces have shaped the design and application of EMR technology, this Part describes the market needs of healthcare providers and then compares and contrasts those needs with the objectives of medical negligence litigation. This Part concludes that EMRs have the unrealized potential to meet the needs of both providers and the judicial system.

16. See *infra* Section III.F.2 for a description of meaningful use incentives. The phrase "meaningful use incentives" refers to the subsidization of EMR systems that have certain functionalities that enhance patient safety and improve quality care. Some of the functions described in this Comment are interoperability, automatic updates, monitoring capabilities, reports, and ease-of-communication.

A. The Role of EMRs in Healthcare

Ensuring safety and quality in healthcare requires that providers accurately, legibly, and promptly communicate with one another.[17] Physicians relying exclusively on paper records notoriously suffer problems arising from illegible handwriting and administrative delays in updating records with lab results.[18] These communication issues can hamper the delivery of healthcare, so providers have shifted away from paper records and toward EMRs.[19]

After looking at the needs of particular entities in the healthcare context, it becomes clear that EMRs are primarily designed to serve the interests of providers. This result is unsurprising given that the primary driving force in EMR designs is market pressure by healthcare providers. Specifically, when looking to purchase an EMR system from one of the more than 1,100 possible vendors, a healthcare provider would look for a number of features that satisfies its needs as a provider and a business.[20]

First, providers need an EMR system that allows them to see the patient as she is at the moment of care. As such, providers need an EMR that permits caregivers to "manipulate" the inputs and access all of the patient's medical information to ensure the data is accurate and up-to-date.[21] An EMR can update automatically to reflect the most up-to-date lab results, vital signs, and diagnoses, permitting the provider to see the patient exactly as she is at the moment of care.[22] EMRs can also alert medical staff if any of a patient's vital signs reach a critical

---

17. *See generally* Committee on Patient Safety & Quality Improvement & Committee on Practice Management, *Patient Safety and Health Information Technology*, AM. C. OBSTETRICIANS & GYNECOLOGISTS, https://www.acog.org/Clinical-Guidance-and-Publications/Committee-Opinions/Committee-on-Patient-Safety-and-Quality-Improvement/Patient-Safety-and-Health-Information-Technology (last visited July 10, 2018) [https://perma.cc/SJE6-NVQ4]; *see also* Peter Garrett & Joshua Seidman, *supra* note 6 (discussing EMRs).

18. *Benefits of Using EHR vs. Paper Records*, CHECKPOINTEHR, https://checkpointehr.com/ehr-vs-paper-records/ (last visited June 11, 2018) [https://perma.cc/EL7T-K2PP].

19. *Id.*

20. *See EHR Adoption Rates*, PRACTICEFUSION (Mar. 1, 2017), https://www.practicefusion.com/blog/ehr-adoption-rates [https://perma.cc/6RAS-349P].

21. *Electronic Medical Records & Electronic Health Records*, OPENCLINICAL, http://www.openclinical.org/emr.html (last visited Mar. 16, 2018) [hereinafter *Electronic Medical & Health Records*] [https://perma.cc/TLA7-8ZRJ].

22. *Id.*

value, facilitating timely responses to emergent conditions.[23]

Second, healthcare providers look for a system that can effectively capture billing items and manage the hospital's inventory.[24] Providers usually operate within business entities and offer healthcare on a fee-for-service basis. From a business perspective, one of the most attractive features of EMRs is the ability to capture billing items and monitor the provider's inventory.[25] An effective EMR system would permit efficient administration of a provider's business needs and ensure the provider is compensated for every service provided. In fact, the first EMRs were designed primarily for this purpose.[26]

Third, the EMR needs to be user-friendly and easily readable. The information on the computer screen should be organized in such a way that a provider can see everything she needs to know. One way that many EMRs make data more accessible to providers is by enabling providers to create "timelines" of health data that show changes in vital signs such as heart rate, respiration, pulse-oxygenation, etc.[27] Analyzing how these values change over time may alert a provider to developing conditions that require attention.

Fourth, EMRs must interface with other EMR systems to facilitate communication between providers, even if those providers have a different EMR system. This function, referred to as "interoperability," allows specialists and other caregivers to contribute previous or developing data to a patient's EMR in such a way that any EMR system could understand the data inputs.[28] Without interoperability, providers' ability to coordinate patient care would be significantly impaired.

Finally, providers have an interest in maintaining and im-

---

23. *Benefits of Using EHR vs. Paper Records*, *supra* note 18.

24. *Id.*

25. *Id.*

26. *See Hospital Information Systems*, EMRCONSULTANT (Aug. 21, 2013), http://www.emrconsultant.com/emr-education-center/emr-selection-and-implementation/hospital-information-systems-his/ [https://perma.cc/66Y3-E232]; *see also* Larry Husten, *Two Dirty Little Secrets About Electronic Health Records*, FORBES (Apr. 12, 2015), https://www.forbes.com/sites/larryhusten/2015/04/12/two-dirty-little-secrets-about-electronic-health-records/#30084a446905 [https://perma.cc/7J3B-D8L4] ("[T]he primary goal of EHRs is to make sure that healthcare providers receive maximum reimbursement and to provide data to executives to help them 'manage' their workers and their systems.").

27. *See Electronic Medical & Health Records*, *supra* note 22 (discussing the need to have immediate access to key information).

28. *Id.*

proving quality and safety at the institutional level. Hospitals in particular benefit from EMR systems that maintain a data trail for quality assurance and peer review purposes.[29] EMRs also enable providers to monitor diseases within the institution, and track overall patient outcomes.[30] Thus, EMRs allow hospitals to see a larger view of how care is being administered within its facilities. A provider purchasing an EMR system will usually look for these features that facilitate patient care, institutional quality, and efficient administration. As a result, most EMR systems are designed to incorporate these features and functionalities.[31]

B. Judicial Interests Implicated in Healthcare Litigation

Medical records, electronic or otherwise, serve entirely different purposes in the context of dispute resolution. Whereas the core objective of healthcare providers is to care for the patient, suits for medical negligence serve the fundamental principle of tort law that "loss from accident must lie where it falls."[32] A provider owes a duty to her patients to provide medical treatment that is consistent with the standard of care. When a provider's treatment is unreasonable, it falls below the standard of care, and an injured party may recover any damages resulting from the breach of that duty. In other words, the goal of medical negligence lawsuits is to compensate patients who suffer injuries resulting from medical treatments that fall below the standard of care.

To prove that a provider acted reasonably or unreasonably, defendant-providers and plaintiff-patients, respectively, must provide details about the *actual* care provided to a patient.[33] Because reasonableness is a holistic analysis, proving reasonableness requires looking at a patient's care over time rather than at any particular moment in time.[34] Moreover, witness

---

29. *Id.*
30. *Id.*
31. *See id.*
32. OLIVER WENDELL HOLMES, JR., *Trespass and Negligence*, *in* THE COMMON LAW 94 (1881 50th prtg. 1923).
33. *See generally* Day v. Johnson, 255 P.3d 1064, 1070 (Colo. 2011) (discussing elements of a medical negligence claim).
34. *See id.* ("Indeed, at times a physician must choose among professionally acceptable alternative diagnoses or therapeutic alternatives and those choices may form the basis for a negligence claim."). The exercise of medical judgment

testimony is often insufficient to recreate the minute details of care. For all these reasons, the medical record is often the best source of evidence in a medical negligence case.[35]

The accuracy of the medical record is critically important to determine fault or non-fault for an injury. On the one hand, an accurate account of the care provided to a plaintiff would fully demonstrate departures from the standard of care by a healthcare provider. On the other hand, accurate and usable records could deter frivolous lawsuits if providers could clearly demonstrate that appropriate care was rendered. At trial, judges and juries benefit from clear and accurate medical records, which allow the focus of the trial to be on the quality and nature of the medical care. Confusing and incomplete medical records are unreliable for evidentiary purposes, and they can damage the credibility of providers who are trying to show a jury that they administered coordinated and prudent care. It is equally true that confusing and unreliable medical records hinder a plaintiff's ability to reach a fair and just result: if the plaintiff cannot effectively demonstrate the actual care given, she cannot demonstrate how that treatment fell below the applicable standard of care. Such outcomes allow negligent providers to escape recognition and accountability. Courts should find this result particularly concerning given that healthcare providers have sole access to and control over the evidence that plaintiffs require to meet their burden of proof.[36]

Similarly, medical records implicate a second interest in judicial economy. Courts as well as lawyers have limited time and resources to manage cases. Courts cannot spend all of their time hearing medical negligence cases or addressing motions that result from technologically induced confusion concerning the EMR. A lawyer, who almost always operates as a business,

---

requires a consideration of all the available facts. For example, a common point of contention in medical negligence lawsuits is whether a physician's differential diagnosis adequately considered the possibility of other causes for a patient's condition. Adjudging the reasonableness of that differential diagnosis requires looking into everything that the physician knew, when she knew it, and whether the physician took adequate steps to gather the appropriate information.

35. FURROW ET AL., *supra* note 3, at 261–62 ("By the time a malpractice action comes to trial memories may have dimmed as to what actually occurred at the time the negligence is alleged to have taken place, leaving the medical record as the most telling evidence.").

36. *See infra* Part IV (discussing the ability to manipulate data to correct errors, and the risk that poses to the authenticity of the record).

has an interest in balancing the costs of discovery against ethical obligations to their clients. A provider, as a party that may have to pay the plaintiff's reasonable costs, also has a financial interest at stake in reducing the cost of dispute resolution. Consequently, courts, lawyers, and litigants all have strong incentives to resolve disputes in the most efficient manner possible. If the medical record provided to the plaintiff is not easily readable or authenticated, then an EMR can contravene that interest in judicial economy.

Finally, the courts play a vital and necessary role in ensuring safe, quality care to patients. In theory, lawsuits for alleged medical negligence accomplish this goal by deterring irresponsible behavior by providers.[37] In practice, however, medical negligence actions do not seem to have any significant, general deterrent effect, even if some evidence tends to show that suits for medical negligence may affect a specific defendant's behavior after-the-fact.[38] That is not to say that medical negligence actions have no effect on quality assurance. Because multiple malpractice suits tend to indicate lower quality care, hospitals can monitor "problem doctors" that may affect the overall quality of care offered at their facilities.[39] Additionally, patients can make more informed choices as healthcare consumers about which providers to use because malpractice liability is usually reported in a national database available to the public.[40] Suits for alleged medical negligence thus play a relatively indirect role in quality assurance. That role is only valuable, however, if the result reached in a particular suit is appropriate based on the merits of the actual medical care provided to the plaintiff.

In sum, although medical providers and the judicial system certainly have different needs with regard to EMRs, those needs are not mutually exclusive. An EMR system should be easily readable and accessible both to providers *and* adverse parties in litigation. Changes and alterations to the record that can be identified by a provider should also be easily identified by non-medical users in litigation. As the next three Parts of

---

37. *See generally* FURROW ET AL., *supra* note 3, at 508–10.

38. *See generally id.* Because they are in the business of helping people, it is likely that doctors, when making decisions, worry more about the patient's well-being than the minute possibility that the patient will sue them.

39. *Id.* at 508.

40. *See What You Must Report to the NPDB*, NAT'L PRAC. DATA BANK, https://www.npdb.hrsa.gov/hcorg/whatYouMustReportToTheDataBank.jsp (last visited June 11, 2018) [https://perma.cc/9CGA-Z6L7].

this Comment illustrate, however, this theoretical possibility is often not realized.

II. THE PRIVILEGE PROBLEM

Before turning to the practical issues surrounding EMRs, the legal authority for the discoverability of an EMR deserves some clarification. In states that substantially parallel the FRCP, discovery in a medical negligence action is generally limited to "any nonprivileged matter that is relevant to any party's claim or defense."[41] A patient should have no difficulty asserting a right to discover her own medical records under FRCP 26(b)(1) and is usually able to admit those records into evidence under the business records exception to hearsay.[42] However, health information is subject to a number of privileges and restrictions that arguably affect the patient's degree of access to an EMR system. Traditional privileges such as the attorney-client privilege and the work product privilege, for instance, apply to the ways a person's health information is used in anticipation of litigation. The manner in which providers use health information for quality control or credentialing may be immune from discovery pursuant to various state statutes governing the peer review privilege even though the underlying health information is discoverable in a medical negligence lawsuit.[43] More relevant here, however, are the restrictions imposed by the Health Insurance Portability and Accountability Act (HIPAA) and the agency regulations—namely, the HIPAA Privacy Rule—promulgated under it. This Part first provides an overview of the HIPAA Privacy Rule before discussing the impact of that Rule on the privileges contemplated by the rules

41. FED. R. CIV. P. 26(b)(1).

42. Kim Baldwin-Stried Reich et al., *Litigation Response Planning and Policies for E-Discovery*, AHIMA (Feb. 2008), http://library.ahima.org/doc?oid=81851 [https://perma.cc/QV9U-YVGZ]. The exception for medical treatment and diagnosis does not fully justify the admissibility of medical records, however, since many of the entries are made for the purpose of billing and inventory rather than for treatment or diagnosis. *See generally supra* Section I.A.

43. FURROW ET AL., *supra* note 3, at 468. As with the work product privilege, the peer review privilege does not immunize the underlying facts from discovery, so the privilege extends only to the peer review proceedings, findings, etc. *See also* Hall v. Flannery, No. 13-CV-914-SMY-DGW, 2015 WL 2008345, at *3 (S.D. Ill. May 1, 2015) (rejecting an assertion of peer review privilege over EMR metadata because the use of the information in scientific study is a question of fact and because the privilege does not extend to the underlying factual information).

of discovery.

A. The HIPAA Privacy Rule

HIPAA was designed to protect the confidentiality of protected health information when a person changes insurance or seeks treatment.[44] The essence of HIPAA is that a patient's identifying health information, referred to by the Act as "protected health information" (PHI), must be kept confidential unless one of a few exceptions applies.[45] Thus any identifying information regarding a patient's care—including the date of care, the fact of care, the reasons for care, and the care provided—is subject to HIPAA restrictions.[46]

The scope of these restrictions is limited by a number of exceptions.[47] The first set of exceptions constitutes the practical exceptions to the HIPAA Privacy Rule.[48] For example, a provider may disclose PHI to qualified persons within a healthcare institution for treatment, payment, and operations purposes.[49] A second set of exceptions applies to "public interest" activities, which expressly permits the disclosure of PHI in judicial proceedings.[50] A third exception permits an individual to request access to her own PHI.[51] Under this exception, an individual may authorize the release of PHI to herself or a designated representative (such as an attorney) with express written consent.[52] A patient's right to access her PHI under HIPAA is not unlimited, however, and hospitals have some discretion to refuse the release of PHI for health or safety purposes.[53]

---

44. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164 (2017)) [hereinafter Modifications to the HIPAA Rules] (discussing enhanced privacy protections under the The Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH is an amendment to HIPAA that clarifies and strengthens the protections of PHI.

45. *Summary of the HIPAA Privacy Rules*, OFFICE OF CIVIL RIGHTS, at 3–4, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last visited Nov. 12, 2017) [hereinafter *Summary*] [https://perma.cc/7AMN-STSF].

46. *Id.* at 4.

47. *Id.* at 5.

48. *Id.*

49. *Id.*

50. *Id.* at 7.

51. *Id.* at 5.

52. *Id.* at 16.

53. *Id.* at 5 ("A covered entity may disclose protected health information to

As a federal statute, HIPAA also has the ability to preempt conflicting state laws that govern the release of information.[54] Put simply, HIPAA provides a floor of protection, and it preempts any state law that offers fewer protections.[55] If a state law affords more protections to the individual, however, the state law controls.[56] Because medical negligence is substantively a tort claim under state law, the release of medical records for discovery purposes potentially implicates HIPAA preemption.

Finally, HIPAA requires that hospitals and other providers disclose only the "minimum necessary" information sufficient to satisfy the needs of any mandated disclosure.[57] HIPAA strongly encourages providers to err on the side of caution when releasing PHI. Disclosing any more or any less than necessary can subject the provider to substantial civil enforcement penalties and even criminal liability under federal law.[58] Consequently, when ordering the release of PHI in whatever form or format, courts must balance the needs of the patient-plaintiff against the potential risks imposed on the defendant-provider.

B. The HIPAA Privilege

Within the framework articulated above, state and federal courts have not clearly delineated the scope of HIPAA's impact on the discoverability of medical records. Furthermore, courts have not taken the opportunity to address the impact of HIPAA on specific EMR functionalities like remote access because that functionality has yet to become regularly accessible to adverse

---

the individual who is the subject of the information."). A situation in which a provider might refuse disclosure would be if such disclosure might compromise the health or safety of the patient.

54. *Id.* at 17.

55. *Id.* ("'Contrary' means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA."). Because one purpose of HIPAA is to provide a means of access to a person's own PHI, state laws which limit the discretion to deny release of PHI to the protected individual would thus survive preemption. *See* Modifications to the HIPAA Rules, *supra* note 44, at 5632.

56. *Summary*, *supra* note 45, at 17.

57. *Id.* at 10.

58. *Id.* at 17–18.

parties in litigation. This Section attempts to determine the impact of HIPAA in those contexts.

Although HIPAA is a limiting factor in the discovery of medical records generally, it does not impose any limitation on the discoverability of a person's *own* medical information. HIPAA should not be read as creating a privilege to a patient's health information that can be enforced against a plaintiff in a suit against the provider, even when that health information exists outside the patient's "legal health record" and may be stored elsewhere in the provider's EMR system.[59] But HIPAA can and should be understood as creating a privilege to other patients' health information that *may* be enforced against the plaintiff-patient unless a court order specifically authorizes access under the judicial use exception. To clarify, consider the following two situations.

In the first situation, a plaintiff believes that the medical record produced by a hospital in response to a discovery request does not contain all of the relevant information. She claims that the record has omitted certain communications between the caregivers and is missing certain video and audio files documenting the care. The plaintiff, with cause, compels the discovery of the medical records in its native format (i.e., the format used by the providers), which would require either on-site inspection of the record or remote access.[60] The defendant argues that it provided the plaintiff with the "designated record set" and that the hospital is precluded from producing any more detailed information because HIPAA permits the hospital to disclose only the "designated record set."[61] The defendant further contends that the Department of Health and Human Services (HHS) has interpreted HIPAA as limiting the forms in which a patient may receive a medical record.[62] Finally, the defendant argues that a patient's right of access is "limited" under HIPAA, which imposes a privilege against

59. The various forms, formats, and locations of health information are discussed *infra* in Part III.

60. *See generally, e.g.*, Borum v. Smith, No. 4:17-CV-00017-JHM, 2017 WL 3014487 (W.D. Ky. July 14, 2017) (describing plaintiff's and defendant's arguments for discovery of the medical record in its native format).

61. *Summary*, *supra* note 45, at 12.

62. *See* Modifications to the HIPAA Rules, *supra* note 45, at 5633 ("We agree with covered entities that individuals should not have an unlimited choice in the form of electronic copy requested.").

discovery of a more expansive record.[63]

The underlying premise of these arguments is that HIPAA does not create a means to enforce a right of access to medical records, but merely outlines the limited procedures by which a patient may request records. Indeed, "critics note that HIPAA standards create little more than a federal confidentiality code based around a regulatory compliance model rather than one that creates patient rights."[64] Although it is true that HIPAA does little to enforce an expanded right of access when a patient requests her medical records for any usual reason, these arguments lack force in the context of the generally accepted concepts of "liberal" discovery.[65] In essence, this is because HIPAA governs only the procedure by which a patient may exercise a right of access; it does not govern the substance of that right.

In fact, the most recent interpretation of HIPAA states that the rule "establishes . . . an enforceable means by which individuals have a right to review or obtain copies of their protected health information."[66] The HIPAA Privacy Rule therefore recognizes a patient's right to access her own information and the ability to enforce that right against a provider. It would be anomalous to conclude that such a statute creates an inverse privilege held by the provider that it can enforce against a patient seeking her own records.

Furthermore, as discussed above, HIPAA carves out an exception for disclosures of PHI in judicial proceedings.[67] HIPAA therefore recognizes a distinction between a patient requesting medical records for personal or business reasons and a patient requesting medical records for the purpose of discovery. For personal or business reasons, a limited medical record set might satisfy a patient's need to have some record of her own care. For purposes of medical negligence litigation, however, a plaintiff-patient would likely need a more thorough and detailed record, which may not always be the "designated record

63. *Id.* at 5632 ("An individual's right of access to an electronic copy of protected health information is currently limited under the Privacy Rule by whether the form or format is readily producible.").

64. FURROW ET AL., *supra* note 3, at 277.

65. A.S. Klein, *Scope of Defendant's Duty of Pretrial Discovery in Medical Malpractice* Action, 15 A.L.R. 3d 1446 § 2 (1967).

66. Modifications to the HIPAA Rules, *supra* note 45, at 5631.

67. *See supra* Section II.A.

set."[68]

The defendants in this first example also argued that a provider retains some discretion in releasing PHI because a patient's right of access is "limited." While it is true that HHS has clarified that the right of access is limited,[69] the context of that clarification is meaningful. The limitation is discussed in terms of pragmatism, where HHS will not require an agency to reproduce the record in a format that is not "readily available."[70] In a statute with so many express limitations on the dissemination of PHI, the absence of an express limitation in the judicial context is significant. Consequently, to the extent that a patient is merely seeking access to her *own* protected health information for the purpose of litigation against the provider, HIPAA should not be interpreted to frustrate the spirit of liberal discovery.

Now consider a second scenario: a plaintiff seeks to prove the defendant-provider's consistent pattern of behavior in similar cases and submits a discovery request for access to other patients' medical records. Here, HIPAA would create a presumptive bar to those records' discovery to the extent that the records contain PHI and the patient to whom that information pertains did not specifically authorize disclosure.[71] The difference between this situation and the first is that the discovery request deals not with a patient's own rights of access but with the confidentiality afforded to other patients' protected information.

Under *these* circumstances, HIPAA and the rules of discovery may conflict. A court faced with this situation may narrowly grant a discovery request in accordance with the "minimum necessary" rule, allowing discovery of the fact of care in other records but omitting from discovery any other personally identifying information. That is not to say, however, that HIPAA provides an absolute bar to the discoverability of other patients' medical records. For example, where a hospital claims that its EMR system malfunctioned, causing records to be lost, the hos-

---

68. *See, e.g.*, Levy v. Patient Hirst of Maryland, Inc., No. 03C12000952, 2012 WL 10703716, at *1–*2 (Md. Cir. Ct. June 11, 2012) (granting plaintiff direct access to the hospital's EMR during depositions); *see also infra* Part IV.

69. Modifications to the HIPAA Rules, *supra* note 45, at 5633. The following two Parts of this Comment discuss how the native file in particular is "readily available" both directly and remotely.

70. *Id.*

71. *See* Klein, *supra* note 65, at § 7.

pital may open the door to a forensic analysis of their system, which would necessitate such extrinsic access to the EMR system and would be permissible under HIPAA's "court order" exception.[72]

To summarize, HIPAA does not restrict access to an EMR in litigation because it does not create a privilege in discovery against expansive access to one's own health information. Rather, the scope of access granted to a patient can and should accommodate the purpose for which the access is sought: for simple disclosures, the usual copy of the designated record set may suffice; for discovery requests, however, HIPAA does not—and should not be read to—create any barrier to the complete discoverability of the facts surrounding a patient's own care. HIPAA and the rules of discovery potentially conflict only when a plaintiff seeks access to another patient's records. Even then, courts are adequately equipped to define a plaintiff's scope of access under the judicial use exception. As such, HIPAA creates no absolute privileges in the discovery of EMRs for medical negligence litigation. With this in mind, this Comment next turns to some of the more practical issues concerning EMR discovery.

III. THE PRODUCTION PROBLEM

Apart from the Privilege Problem, the discoverability of medical records is further limited by requirements of relevance[73] and format, especially in the context of e-discovery.[74] A piece of evidence is relevant if it "has any tendency to make a fact more or less probable than it would be without the evidence."[75] In matters concerning medical care and treatment, even the most minute details can make alleged negligence "more or less probable." That need for a thorough and detailed inquiry is one reason why judges have afforded such liberal discovery of medical records.[76]

Recovering these minute details can be incredibly difficult

72. *Summary*, *supra* note 46, at 7.
73. FED. R. CIV. P. 26(b)(1).
74. FED. R. CIV. P. 34.
75. FED. R. EVID. 401(a). Note that in the discovery context, the standard of "relevance" is broader than the standard of "admissibility, so even inadmissible evidence might be subject to discovery.
76. *See infra* Part II.

under the current design of EMR systems. Perhaps the most daunting problem in e-discovery of medical records is ordering the production of the medical record in a format that both satisfies the requirements of the FRCP *and* facilitates meaningful discovery by both parties.[77] This Part first discusses the variety of options by which a responding party may produce the requested medical record. Then this Part discusses the general problem of definition inherent in the Production Problem. Finally, this Part compares the HIPAA rules governing form and format with the proportionality analysis under the 2015 amendments to the FRCP and dispels any notion that HIPAA and the FRCP actually conflict.

A. Possible Forms and Formats of the Medical Record

As mentioned briefly in Part I, providers have several options available when responding to a request for production.[78] First, the provider could print the medical record in hard copy form, with all relevant fields expanded.[79]

Second, the provider could reproduce the record in a digital format.[80] This digital record could represent either the "legal health record" or the "designated record set" depending on the purpose for which it is being produced.[81] For example, in a HIPAA production, patients would receive the designated record set, which contains all protected health information, including billing, insurance, and other identifying information.[82]

---

77. For simplicity's sake, this article refers to the rules of civil procedure applicable in actions alleging medical negligence as the FRCP even though these actions are almost always governed by state procedural laws. Given that the vast majority of state rules of civil procedure substantially or completely reflect the federal rules, this decision should not be problematic.

78. For a more detailed discussion of the pros and cons of each of these forms and formats, *see* Jeffrey L. Masor, *Electronic Medical Records and E-Discovery: With New Technology Come New Challenges*, 5 HASTINGS SCI. & TECH. L.J. 245 (2013).

79. EMRs usually record certain events on a minute-by-minute basis, but a printout may display the information in, for instance, five-minute intervals, thus shielding the more precise information from the requesting party. This approach also has the disadvantages of not appearing in a readable format (as discussed in Part I).

80. Mary Beth Haugen et al., *Fundamentals of the Legal Health Record and the Designated Record Set*, AHIMA (Feb. 2011), http://library.ahima.org/doc?oid=104008 [https://perma.cc/Q269-WBNN].

81. *Id.*

82. *Id.*

More relevant here is the legal health record, which is a narrower record extracted from the native EMR that contains only the information "used by the patient care team to make decisions about the treatment of a patient."[83] The legal health record usually constitutes the provider's official business record of care and, in theory, should contain every piece of relevant information.[84]

Finally, a patient's health record exists in its native format on the provider's electronic systems and can be accessed by authorized persons within the healthcare institution at any time during the course of litigation. These authorized persons have the full ability to see the information in a readable format and even have the full ability to modify the record.[85] With these general options in mind, we turn next to what the FRCP require during discovery.

B. Defining "the" Medical Record

Defining the medical record for the purposes of litigation is always a point of contention in discovery. To adequately meet their respective burdens, litigants on all sides require a record that accurately reflects the entirety of the care actually given. When a plaintiff receives a print-out or PDF version of the record, it is nearly impossible to determine whether that record is complete. In other words, if a plaintiff has not received the native record, that plaintiff does not know what information, if any, has been omitted.

For example, in *Donato v. Nutovits*[86] the plaintiff's lawyer discovered omissions while taking depositions and comparing contradictory affidavits. The plaintiff then received four different PDF versions of his deceased wife's medical file after four successive discovery requests, and each of those versions provided the plaintiff with different information.[87] The discovery dispute in *Donato* is fairly typical in cases involving reproduced

83. *Id.*

84. *Id.* Notably, the legal health record often does not contain every minute detail, and the process of reproducing the medical record into a static format often corrupts some of the data or renders it unreadable. So, in practice, potentially relevant information is often omitted in the legal health record. *See generally* Masor, *supra* note 79.

85. *See infra* Section III.C.

86. No. 70468/2012, 2016 WL 9738291, at *1 (N.Y. Sup. Ct. Apr. 7, 2016).

87. *Id.* at *2.

records because no single form or format of the reproduced medical record contains all relevant information in every case.[88] Although HIPAA and several state laws define the medical record as whatever information was used by the care team in treating a patient,[89] not all of that information may be available in a digital copy of the record.

For example, several EMR systems have a "sticky note" function that permits providers to communicate between shifts.[90] Those notes are not viewable on the legal health record but may be viewable in the native format.[91] Furthermore, video or audio files that may be stored in the native record will probably not be reproduced in the legal health record, but may be accessible in the native file.[92] One compelling reason that providers omit these files from the legal health record is that it can be traumatic for some patients to see or hear the details of an operation. A patient requesting a record for insurance purposes, for example, would not need to see such graphic and disturbing content, so a written report would normally suffice under the "minimum necessary" requirement of HIPAA.[93] However, litigation needs are different from the usual business uses of a legal health record: in litigation, inquiries are more fact specific and authentication is paramount. Video or audio files therefore could contain discoverable information that is relevant to a party's claims or defenses but may not be in the legal health record.

Finally, the legal health record may be accompanied by an "audit trail," which shows whether and when something in the record changed and who changed it but usually does not show

---

88. *See infra* Part IV.

89. For a fairly exhaustive list of state statutes that grant patients a right to their health information, *see* Karl A. Menninger, II, *Confidentiality of Medical and Other Treatment Records*, *in* 87 AM. JUR. PROOF OF FACTS 3D 259 § 15 nn.1–6 (2006, Oct. 2018 Update).

90. *See 2012 Ambulatory Provider Brochure*, LANCASTER GEN. HEALTH, http://www.lancastergeneralhealth.org/LGH/ECommerceSite/media/LGH-Media-Library/Documents/Healthcare%20Professionals/2012_Ambulatory_Provider_Brochure_1.pdf (last visited June 11, 2018) [https://perma.cc/2V8Y-5B4H] (discussing features of Epic Systems' EMR).

91. *See, e.g.*, *Donato*, 2016 WL 9738291, at *2 (plaintiffs learned in deposition that nursing notes were missing from the record provided to them in response to a discovery request).

92. *See supra* Section III.A.

93. *See supra* Part II (discussing the minimum necessary requirement of the HIPAA Privacy Rule).

how that data was changed.[94] Because the records are so malleable, it can be difficult for parties to know what data reflect care that was actually given versus what care, in retrospect, should have been given.[95] This effort becomes particularly difficult when plaintiffs have to interpret the record using an audit trail that lacks a clear "track changes" functionality. Post-care edits without a proper audit trail may be presented as actual medical care in the absence of a method for maintaining data integrity. As a result, plaintiffs will require the assistance of multiple (and expensive) experts to decipher their own records. While the audit trail is not part of the legal health record, it is independently discoverable in most cases.[96]

These problems should inform a court's analysis under the FRCP requirement that a party be able to "inspect, copy, test, or sample"[97] any electronic information "stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."[98] On its face, the FRCP permit discovery of all three forms of an electronic health record: a print-out would be permissible if it was "reasonably usable;" an electronic copy of the legal health record would be permissible "if necessary, after translation;" the native file, finally, could be accessed "directly."[99]

The requesting party also has the power to "specify the form or forms in which electronically stored information is to be produced."[100] Absent that specification, a party must produce the documents "as they are kept in the usual course of business."[101] In the context of discovery in medical litigation, this second phrase is particularly unhelpful because providers "keep" their medical records in two formats in the usual course of business (the native file and the legal health record), and the FRCP provide no guidance on which format operates as the floor.

Naturally, the requesting party will want as much access

---

94. *See* Masor, *supra* note 79, at 254; *see also infra* Section IV.B.
95. *See* FURROW ET AL., *supra* note 3, at 262.
96. *See, e.g.*, Borum v. Smith, No. 4:17-CV-00017-JHM, 2017 WL 3014487 (W.D. Ky. July 14, 2017) (granting plaintiffs access to defendant's audit trail).
97. FED. R. CIV. P. 34(a)(1).
98. FED. R. CIV. P. 34(a)(1)(A).
99. Subject to the limitations discussed in *infra* Section III.C.
100. FED. R. CIV. P. 34(b)(1)(C).
101. FED. R. CIV. P. 34(b)(2)(E)(i).

to the record as possible, and a savvy defendant will always want to limit the ability of a party to directly access its systems. Because of these opposing objectives, disputes often arise over the form, format, and total content that a party must produce. However, since FRCP 34 provides little guidance on the scope of a party's obligation to produce medical records in response to a discovery request, litigants must turn to FRCP 26 to delineate the scope of discovery.

C. Proportionality Analysis Under the FRCP

As explained above, the relative access to information in medical negligence litigation is currently weighted heavily in favor of the provider. A provider has complete access to the native EMR, while the plaintiff-patient has access only to what the provider has given her in response to a discovery request. This Section attempts to clarify the appropriate scope of discovery under the current 2015 amendments to the FRCP.

Courts resolving discovery disputes must balance a number of "proportionality" factors in tandem with the privilege and relevance limitations.[102] Specifically, the scope of discovery under the current FRCP must be:

> proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in discovery, the parties' relative access to information, the parties' resources, the importance of discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.[103]

Compared to the previous reasonably-calculated standard, this new proportionality test provides more specific guidance to judges by emphasizing pragmatism and fundamental fairness, especially given the prevalence of e-discovery in litigation. Of particular importance here are the factors of access, resources, importance, and expense. When a court is determining which form of the medical record a party should produce or whether the court should grant a party direct access to the provider's system, the scope of discovery will turn on these four factors.

---

102. FED. R. CIV. P. 26(b)(1).
103. *Id.*

First, courts must consider each party's "relative access" to information. As the custodian of the medical record, a provider has complete access to the EMR in its native format for the entire duration of litigation.[104] Incidental to this direct access is the ability to manipulate the information to produce timelines, see patient notes, delete unfavorable information, and access other functionalities that exclusively operate in the native format. A patient, however, has access only to what the provider provides her, and the form of the medical record is often confusing, unreadable, and visually different than it is in the native format.[105] Because of this obvious imbalance, courts may feel the need to grant direct access to the native file as a matter of fundamental fairness. Of course, direct access may not be necessary in all cases, and orders must be tailored to the facts of each case.

Second, providers have significantly greater resources than plaintiffs in most cases, prompting courts to take steps to guarantee the authenticity and completeness of the record produced by the provider. Setting aside the disparity in financial resources, providers have complete power over the record, including the ability to change it at any time.[106] Because EMRs are designed to be changeable, the risks inherent in the temptation to alter records must be taken into account when making a discovery plan.[107] Should a court decide that access to the native

104. The scope of a mid-level provider's access to the EMR is usually a heavily litigated issue. Some states, such as Colorado, permit a hospital to access the entire native record when the hospital is sued because the physician-patient privilege is waived with respect to the hospital when the patient sues that hospital. *See* Ortega v. Colo. Permanente Grp., 265 P.3d 444, 446 (Colo. 2011). However, a physician cannot access the native record without authorization from the plaintiff because the privilege against the physician has only been waived for the care at issue in the litigation. *See* Alcon v. Spicer, 113 P.3d 735, 741 (Colo. 2005). Despite that technicality, physicians and other mid-level providers will usually receive that authorization to access the native record at some point during the litigation as a practical matter because FRCP 12—and its state equivalents—requires that documents be made available to the opposing party.

105. Ralph C. Losey & Kristen A. Foltz, *Electronic Medical Records: What Are Some of the Practical Issues Lawyers Should be Aware of During Discovery and Litigation?*, 5 A.B.A. HEALTH ESOURCE, No. 10, June 3, 2009, https://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/Losey.html [https://perma.cc/A8RW-CACH].

106. *See infra* Part IV.

107. *See* Anthony C. Casamassima, *Spoliation of Evidence and Medical Malpractice*, 14 PACE L. REV. 235, 236–37 (1994) ("It has been estimated that as many fifty percent of medical malpractice cases involve altered records, and that ten percent of all malpractice cases involve fraudulently altered records.").

file is not necessary in a particular case, the court could still address this concern by granting access to an audit trail which verifies the authenticity of the record. In fact, the current trend has been to grant access to an available audit trail regardless of whether the authenticity of the record is in question.[108]

Third, the importance of the record favors direct access. In a medical negligence lawsuit, the record is the most important piece of evidence because it details the course of care at issue in the case.[109] Because the native file is more readable and user-friendly and because it is the very format used "in the usual course of business," providers will always have an easier time preparing for depositions than plaintiffs will. However, because a printed reproduction of the record is visually different from the native file, nurses and doctors in depositions may have a hard time interpreting a PDF or print-screen version of the record, which can draw out a deposition or even require multiple depositions.[110] Beyond these practical concerns in judicial fairness and efficiency, the native file may have audio or video files that document diagnostic or treatment information in real time. Access to these files would obviously be invaluable to the judicial interest in accurate factfinding. When such information is available, the mere summaries of care in the legal health record may be insufficient to satisfy judicial interests in cases involving the minute details of care.

Although the previous three factors tend to favor a requesting party's direct access to the record, the fourth factor, burdens, cuts both ways. Whereas producing a print or electronic copy of the record can be very expensive and would thus favor direct access, courts must also take the costs of storage and storage capacity into account, which could cut *against* direct access in certain circumstances. For example, reproducing

---

108. *See, e.g.*, Moan v. Mass. Gen. Hosp., No. 15-CV-1122-H, 2016 WL 1294944, at *1 (Mass. Mar. 31, 2016) (granting plaintiffs access to the audit trail); Baker v. Geisinger Cmty. Med. Ctr., No. 16 CV 2946, 2017 WL 1293251, at *1 (Pa. Com. Pl. Apr. 7, 2017) (audit trail was relevant to the claims at issue and was therefore discoverable); Gilbert v. Highland Hosp., 31 N.Y.S.3d 397, 400 (N.Y. Sup. Ct. 2016) ("[S]ystem metadata is relevant, however, if the authenticity of a document is questioned *or if establishing who received what information and when is important to the claims or defenses of a party*." (quoting Aguilar v. Immigration & Customs Enf't Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 354 (S.D.N.Y. 2008))).

109. FURROW ET AL., *supra* note 3, at 261–62.

110. *See* Losey & Foltz, *supra* note 106.

the native file into a separate document is an arduous task that is usually more effort than it is worth.[111] Such burdens could be avoided by granting direct access, but providers also have an interest in protecting the confidentiality of their records, a burden that must be considered against the practical benefit of unencumbered access to a provider's EMR system.[112]

Even then, direct access may be less burdensome for both parties in some cases when compared to the burdens imposed by a paper or PDF reproduction of the record. Interpreting a post hoc translation of the record will require plaintiffs to hire experts who can interpret this unique form of the record, to cross reference that record with the audit trail, and to ultimately recreate that information in a presentable format. This reconstruction of the record, which may be thousands of pages, always burdens the plaintiff more than the defendant because the provider always has the native file readily available. Therefore, each alternative potentially imposes significant costs on each party, both in terms of time and money, which will invariably create a balancing act unique to each case.

Finally, FRCP 26(b)(1) requires that those costs be balanced against the potential benefits to the parties.[113] Paper records or electronic copies certainly have some benefits. Paper records are static documents that can be easily copied and taken anywhere, and they do not carry the security risks inherent in direct or remote access to the record. However, the native format also has its advantages. Deponents involved in the plaintiff's care will have a familiar format of the record in front of them, allowing for more effective depositions.[114] The native format also permits parties, including nurses and physicians, to see the specific details of care, enabling more effective preparation in advance of trial and limiting surprises by either side. In the context of discovery, the FRCP's proportionality factors

111. *See, e.g.*, Peterson v. Matlock, No. 11-2594 (FLW)(DEA), 2014 WL 5475236, at *2 (D.N.J. Oct. 29, 2014) ("Although the PDF record provided may be less convenient for Plaintiff, requiring staff from the DOC to sort and identify each page of every inmate medical record would create a substantial hardship and/or expense, which outweighs Plaintiff's interests in receiving the medical records in their native format.").

112. See *infra* Section III.F, which discusses practical means to limit direct access to accounts for privacy and security concerns.

113. FED. R. CIV. P. 26(b)(1).

114. *See* Levy v. Patient Hirst of Md., Inc., No. 03C12000952, 2012 WL 10703716, at *3 (Md. Cir. Ct. June 11, 2012).

certainly favor more expansive access to the complete record in its native format, and that has been the general trend in courts that have tackled the question.[115]

D. HIPAA Rules Governing Form and Format

As mentioned in Part II, HIPAA is always implicated where the disclosure of health information is involved. Here, two questions arise. The first is whether HIPAA permits a provider to disclose health information besides that contained in the designated record set. The second is whether HIPAA permits direct or remote access to a provider's EMR database for discovery purposes.

Turning to the first question, HIPAA has never been interpreted as limiting an individual's right of access to her own PHI, except where such access may endanger the individual or others.[116] Concerns about an individual's imminent health and safety are rarely relevant in the discovery context, so that exception would not apply. Even then, HIPAA provides an express exception for the release of PHI for judicial purposes.[117] HIPAA therefore permits providers to disclose all of a patient's health information to that patient, even if that information is not contained in the provider's designated record set or legal health record. Courts should thus easily dispense with this first question.

The second question is more complicated. HHS has stated that providers "are not required by HIPAA to provide individuals with direct access to their systems."[118] Providers will often invoke this language to contend that they have no duty to provide litigants with direct access and attempt some form of HIPAA preemption analysis, arguing that the more "stringent" standard under HIPAA controls.[119]

When patient access is at issue, preemption analysis is not so simple. Because one of the secondary objectives of HIPAA is to "aim to give consumers control over their own health infor-

---

115. *See, e.g.*, Griffin v. Univ. of Md. Med. Sys. Corp., No. 24-C-15-004716, 2016 WL 8739727 (Md. Cir. Ct. Sept. 26, 2016).

116. *See Summary*, *supra* note 46, at 21 n.57.

117. *Supra* Section II.A.

118. Modifications to the HIPAA Rules, *supra* note 45, at 5631.

119. *Id.* at 5576–77 (discussing preemption analysis generally and concluding that state law controls only if it provides more stringent protections of PHI than HIPAA does). *See also supra* Section II.A.

mation,"[120] HIPAA exempts state laws from preemption if they "provide greater . . . privacy rights."[121] HHS has interpreted HIPAA preemption such that "[i]n the case of right of access, more stringent means that such State law permits greater rights of access to the individual."[122] While it is true that HIPAA does not require direct access, it likewise does not foreclose that possibility when the individual is looking exclusively at her own information. Thus, HIPAA does not preempt state discovery rules that permit a plaintiff-patient's direct access to a defendant-hospital's EMR systems.

E. Going Fishing?

While direct access to EMR systems may best fit the proportionality standards in FRCP 26(b)(1) and may not necessarily be preempted, direct access does come with several risks that implicate HIPAA and may expose a hospital to liability. For example, an EMR system may lack a "read-only" functionality that prevents a user from making changes to the health records, or it may lack any meaningful way to limit a user's access to other patients' records.[123] Given the risk to other patients' protected information in such circumstances, HIPAA may actually afford greater protections than unbridled direct access to EMR servers.

Additionally, courts have been hesitant to grant plaintiffs complete access to defendants' electronic systems due to concerns about "fishing expeditions"[124] in which an overzealous plaintiff rummages through a defendant's files for information that is not necessarily discoverable, thus unwarrantably invading the defendant's privacy. A commonly cited example that expresses courts' aversion to such expansive discovery is *In re Ford Motor Co.*, a products liability case.[125] There, a plaintiff requested direct access to Ford's databases to conduct a search for other claims similar to his own claims.[126] Because the plaintiff requested unrestricted access to the defendant's computer

120. FURROW ET AL., *supra* note 3, at 468.
121. *Summary*, *supra* note 46, at 17.
122. Modifications to the HIPAA Rules, *supra* note 45, at 5632.
123. *See generally* Mason, *supra* note 79.
124. *See* Hickman v. Taylor, 329 U.S. 495, 507 (1947).
125. 345 F.3d 1315 (11th Cir. 2003).
126. *Id.* at 1316.

systems without establishing parameters for the search, the court denied direct access to Ford's databases.[127]

Despite any usefulness the decision may have in the context of e-discovery generally, *In re Ford* provides little guidance in the EMR context for several reasons. Unlike with EMRs, the database at issue in *Ford* involved static documents that could be made available in a usable, printable format. Furthermore, healthcare providers—unlike car manufacturers—have a legal duty to disclose a patient's medical information to that patient upon request.[128] Finally, *In re Ford* is easily distinguishable from EMR cases because it involves a products liability claim rather than a professional liability claim.

Perhaps a better standard was articulated in *Hickman v. Taylor*, where Justice Murphy elaborated upon the spirit of discovery before electronic information created so many complications:

> We agree, of course, that the deposition-discovery rules are to be accorded a broad and liberal treatment. No longer can the time-honored cry of 'fishing expedition' serve to preclude a party from inquiring into the facts underlying his opponent's case. Mutual knowledge of all the relevant facts gathered by both parties is essential to proper litigation. To that end, either party may compel the other to disgorge whatever facts he has in his possession. . . . But discovery, like all matters of procedure, has ultimate and necessary boundaries. As indicated by Rules 30(b) and (d) and 31(d), limitations inevitably arise when it can be shown that the examination is being conducted in bad faith or in such a manner as to annoy, embarrass or oppress the person subject to the inquiry. And as Rule 26(b) provides, further limitations come into existence when the inquiry touches upon the irrelevant and encroaches upon the recognized domain of privilege.[129]

In the quoted passage, Justice Murphy attempts to draw a line between fair discovery, which furthers the quest for truth, and abusive discovery, which seeks only to harm the opponent.

---

127. *Id.* at 1317.
128. *See supra* Part II.
129. *Hickman*, 329 U.S. at 507–08

While Justice Murphy certainly could not have contemplated the enigma of e-discovery, the fundamental spirit of discovery as furthering the judicial interests in accurate factfinding and fair outcomes survives to this day.[130] To further those interests, both parties should have equal access to whatever information is necessary to prevent surprise and to properly, fairly, and accurately adjudicate a claim. The beauty of such a standard is its inherent flexibility. Although a legal medical record may suffice in one case, more expansive discovery, such as granting some form of direct access, may be necessary in others.

Such determinations may turn on the phrase "if necessary,"[131] requiring courts to ask whether effective discovery—including effective depositions—requires direct, remote access to the native file. To illustrate this balancing act, consider the following cases. In *Peterson v. Matlock*,[132] the court denied a plaintiff's motion to compel discovery of the plaintiff's medical record in its native format because the request was unduly burdensome.[133] There, the plaintiff did not request direct or remote access to the defendant's EMR system, but instead requested that the defendant reproduce the native record in an exportable format.[134] The plaintiff argued that the PDF record was not searchable, was fragmented, and was difficult to navigate.[135] The defendants argued that the record, although inconvenient for the plaintiff, was the "standard output and method of production" supplied to plaintiffs.[136] Rather than finding that the plaintiff's discovery request was too expansive, the court concluded that the effort required of the defendant to replicate the native record was simply too burdensome in light of the marginal benefits.[137]

Unlike the *Peterson* court, the court in *Griffin v. University of Maryland Medical Systems Corp.* granted a plaintiff on-site access to the defendant's EMR system to inspect the plaintiff's

130. Interestingly, Justice Murphy's formulation of the bounds of discovery mirror FRCP 26(b)(1), which most recently includes the proportionality analysis that emphasizes fair and equal access to information.

131. FED. R. CIV. P. 34(a)(1)(A).

132. No. 11-2594 (FLW)(DEA), 2014 WL 5475236 (D.N.J. Oct. 29, 2014). Notably, this case arose before the FRCP proportionality factors came into effect.

133. *Id.* at *3.

134. *Id.* at *1.

135. *Id.*

136. *Id.*

137. *Id.* at *2.

medical record.[138] In *Griffin*, amidst a contentious discovery process, the defendant had produced five revisions of the medical record, which the plaintiff claimed were not responsive to her discovery requests.[139] The plaintiff desired the ability to search the entire medical record for the term "preeclampsia" but could not do so in the forms produced.[140] Because the defendant was unable to articulate any burden that resulted from permitting on-site access, and because the plaintiff set specific parameters for access, the court rejected the defendant's argument that the discovery request was a "fishing expedition."[141] The court then granted supervised on-site access for an expert to inspect the defendant's EMR system.[142] Notably, if the plaintiff had had such access from the beginning of discovery, the five additional requests for production would not have been necessary. In this way, *Griffin* illustrates a paradox of EMR discovery that distinguishes it from other discovery contexts. Whereas a broader scope of discovery in some contexts—namely, the infamous "document dump"—could impose insurmountable burdens on the party seeking discovery, the exchange of a larger volume of information through direct access actually saves both a litigant's time and a court's judicial resources.

As courts continue to confront the developing problems of EMR discovery, supervised on-site access may be the most reasonable option in light of the currently available alternatives. Exporting a native record in some reproduced form is significantly more burdensome than on-site access, at least for defendants. Consequently, when disputes arise over the adequacy or usability of the record, courts may continue to grant supervised on-site access.

F. Possible Approaches to Authorizing Direct Access

To briefly summarize the thrust of this Part so far, the current discovery regime set forth in the FRCP and marginally affected by HIPAA permits plaintiffs in many cases to have direct access to the record. However, EMRs are not currently

138. No. 24-C-15-004716, 2016 WL 8739727 (Md. Cir. Ct. Sept. 26, 2016).
139. *Id.* at *1.
140. *Id.*
141. *Id.* at *2.
142. *Id.* at *3.

designed to facilitate access for the limited purpose of discovery. For external users, EMRs may not have a "read-only" function and may not have the ability to limit user privileges to a single patient's record. Direct access therefore comes with the risk that plaintiffs will either intentionally or inadvertently access other patients' records and thus breach a provider's duty of confidentiality under HIPAA or state law. With these risks, benefits, and burdens in mind, this Section discusses a number of alternative solutions to the Production Problem.

1. Proposal 1: Permit Supervised Direct Access to the Provider's EMR Systems

As previously discussed, one proposed solution available to courts is to permit the plaintiff to have supervised direct access to the provider's EMR system. Although this proposal addresses some of the concerns of the Production Problem, it is not a complete solution. The consequence here is that both parties are ultimately burdened by necessary safeguards in cases for which direct access is warranted. Because providers bear the risk of breach, direct access by a plaintiff will likely be supervised by the provider, which requires the provider to monitor and verify everything a plaintiff accesses. This supervision is inconsistent with the general principles behind the work product privilege because providers can potentially infer litigation strategies from how a plaintiff inspects the record. To offset that risk, plaintiffs might be encouraged to use some stealth and misdirection, intentionally conducting searches into irrelevant parts of the record, knowing that the opposing party is watching over their shoulder. The result, then, is that both parties expend valuable time inspecting the record on-site, and the inspecting party does not have the common protections of work product privilege.

2. Proposal 2: Update the Meaningful Use Requirements to Require a Remote, Read-Only Function for Purposes of Litigation

As explained above, the federal government encourages the adoption of EMR systems through an EMR incentive program

under Medicare and Medicaid.[143] Providers receive those subsidies, however, only if an EMR system satisfies the program's meaningful use requirements.[144] Although participation in the program is voluntary, Medicare and Medicaid providers who do not take meaningful steps to comply with the "meaningful use" requirements receive a negative adjustment to their Medicare and Medicaid fees.[145] Because Medicare and Medicaid, together, are the largest payers of healthcare, these incentives have substantial force in encouraging the adoption of EMRs with specific functions.[146]

The federal government should update Medicare's meaningful use requirements to make EMR systems more responsive to the needs of dispute resolution, permitting legitimate claims to reach a prompt conclusion while dispensing illegitimate claims with minimal cost. To achieve that goal, EMR systems would need to include remote-access and track-changes functions. By subsidizing these functions as meaningful uses, hospitals would not have to bear the full cost of any software updates or other system changes. Moreover, hospitals that wish to purchase EMRs without these functions could choose to do so, but their EMR expenses would not be subsidized by Medicare and Medicaid.

As with any plan involving health information, such a solution is not without risks. For example, including a remote-access function poses a number of security and privacy concerns. First is the risk that an adverse party could remotely alter the record to their benefit. Just as providers may be tempted to cover up mistakes, so too may adverse parties attempt to amend the facts to strengthen their cases. While one solution to that risk is to solidify an EMR's track-changes function, the strongest safeguard against such intrusions is to "freeze" the record by making remote access read-only. That way, plaintiffs and defendants could view the record as it appears in the normal course of business but could not alter it.

Second is the risk of a data breach. During discovery, a

143. *Meaningful Use: Introduction*, CDC, https://www.cdc.gov/ehrmeaningfuluse/introduction.html (last visited June 11, 2018) [https://perma.cc/K343-FPVY].

144. *Id.*

145. *Id.*

146. *See generally* TEVI D. TROY, AM. HEALTH POL'Y INST., HOW THE GOVERNMENT AS A PAYER SHAPES THE HEALTH CARE MARKETPLACE' (2015), www.americanhealthpolicy.org/Content/document/resources/Government_as_Payer-12012015.pdf [https://perma.cc/L8QG-TZXS].

plaintiff should have access to an EMR system only to the extent necessary to litigate her claim. In general, that would require viewing only her own record and would not warrant unbridled, remote access to the entirety of the provider's EMR system. That degree of access would amount to a forbidden fishing expedition and would not be proportional to the needs of discovery. Therefore, an EMR that permits remote access should provide a means of limiting that access to approved patients in accordance with a court order and in compliance with HIPAA's minimum necessary rule.

3. Proposal 3: Create a Presumption That the Native Record Be Remotely Available to All Parties in the Litigation

The overriding theme of this Comment is that obtaining medical records for litigation is a tremendous burden for all parties involved. Plaintiffs will always grapple with problems of authenticity, completeness, usability, and readability when attempting to obtain and interpret records. Providers may also have to litigate the scope of the physician-patient privilege as it applies to the medical record, creating unnecessary and costly peripheral issues for a medical negligence case.

For example, in Colorado, a hospital or other healthcare institution sued by a patient has access to a patient's *entire* medical record in its native format because the patient has impliedly waived the privilege by suing the hospital, because the hospital owns the EMR system, and because the entire *unredacted* record is relevant to claims and defenses.[147] Physicians and mid-level providers who contract with a hospital, however, still only have the benefit of a limited waiver and have not been granted such uninhibited access unless either the hospital or the plaintiff provides that unredacted record.[148] As a result, the plaintiffs and defendants most severely affected by medical

147. Ortega v. Colo. Permanente Grp., 265 P.3d 444, 446 (Colo. 2011).

148. *See* Alcon v. Spicer, 113 P.3d 735, 741 (Colo. 2005), *modified* June 27, 2005 ("To comply with the privilege statute, the order should have been tailored to the scope of the waiver of the physician-patient privilege, meaning it should have been tailored to the injuries and damages claimed . . . ."). It is notable that physicians may still physically access the record and make changes if they have a log-in and password for the hospital's EMR system. This access would constitute a data breach under HIPAA and would subject the physician and the hospital to potential civil and criminal liability.

negligence litigation must fight to obtain the complete, usable record and therefore must fight to obtain the best evidence to support their claims or defenses. Such a result is surely violative of the spirit of discovery under the FRCP proportionality analysis.

Courts could remedy this situation by creating a presumption that all parties in medical negligence litigation should have direct or remote access to the entirety of the medical record. Such access would facilitate freer inspection of the record by all parties, thereby preserving litigants' work product privilege to a greater extent than would supervised direct access.[149] Plaintiffs and non-hospital providers could access hyperlinks to changed data points, access audio files, see nursing notes, and generate timelines, none of which is possible from the PDF record. At trial, litigants on all sides could enter screenshots of the medical record into evidence in the same form and format, thereby placing all parties on an equal playing field throughout the entirety of litigation.

This remote-access function would also reduce the time spent authenticating the record by eliminating the need for successive discovery requests and re-depositions when a party notices that a produced record is incomplete. Litigants on all sides of a deposition, for example, would have an easier time discussing the facts described in the record if that record were available in a format familiar to the providers. The providers could then discuss the medical record without the need for additional preparation, avoiding a potentially awkward situation in which a provider would have to explain to a jury that she does not understand the record.

As with Proposal 2, this remote-access function carries security and privacy risks that must be addressed. Until and unless EMR vendors develop a read-only function for litigation purposes, courts will have to take steps to protect the integrity of the record and prevent abuse of the information. Courts could deter such abuses by placing a protective order on the

149. As discussed *infra* in Part IV, many EMR systems do have an audit trail that shows who accesses the record, when they accessed it, and what they saw. Because many audit trails also show who accessed the audit trail, courts could include in a protective order that providers shall not inspect the audit trail for the purposes of tracking another party's work product, whether that party be the plaintiff or another adverse defendant. The court could inspect the audit trail where necessary and impose sanctions where appropriate.

record and clearly establishing the parameters for inspecting it. A violation of this protective order would subject the noncompliant party to appropriate sanctions, such as requiring the defendant to provide HHS with a written notice of its HIPAA violation and awarding the plaintiff attorney's fees. These orders should relate to both the scope and authenticity of the record. Of course, courts should sanction any party that intentionally alters the record in an effort to fabricate information. However, an inquiry into a patient's sensitive medical history—such as a history of sexually transmitted diseases or abortion—for purposes of besmirching a victim's character should not be permitted during discovery. Such activity should also be proscribed by a protective order.

Although the effects of this proposal would expand the discoverability of EMRs to the benefit of plaintiffs and physicians but to the strategic detriment of hospitals, this Comment's larger argument is that the available short-term solutions are not desirable in the long run for any party. Proposed solutions should work to the benefit of all sides. Unless and until Congress or CMS decides to update the meaningful use requirements, courts should adopt Proposal 3: permitting remote access under a protective order. This proposal best balances the needs of litigation against the legitimate security and privacy interests inherent in PHI disclosures, and it simplifies the discovery process for both plaintiffs and providers.

IV. THE PRESERVATION PROBLEM

Turning to the final issue raised in this Comment, EMRs are particularly difficult to preserve for litigation compared to more static forms of electronic information. Meaningful discovery—and thus efficient dispute resolution—requires that both parties have a complete record that accurately reflects the actual care provided to a patient. In turn, accurate fact-finding requires that this record be preserved during the course of litigation.

The provider's duty to preserve raises some unique questions in the context of EMR discovery. For instance, because EMRs are "abstractions"[150] (rather than static documents) and

150. Robert J. Hudock & Jason E. Christ, *Electronic Health Records Pose Several Challenges*, EPSTEIN BECKER GREEN (Dec. 14, 2009), https://www.ebglaw

are designed to be manipulated,[151] one issue relates to the safeguards necessary to ensure that a party being sued cannot deceptively or fraudulently alter the record. Moreover, EMR software is often managed by a third party, usually the producer of the software who controls updates.[152] Because those updates may alter how information is displayed or may destroy that information entirely, another issue involves the extent of the provider's duty to preserve in light of that known risk of losing data. Finally, hospitals and other providers have more than one preservation duty. Aside from the common law duty to preserve discoverable materials in anticipation of litigation,[153] providers also have a statutory duty to preserve all records under Medicare.[154] Although a provider may be tempted to believe that the duty to preserve is satisfied solely by compliance with Medicare, the common law duty to preserve evidence in anticipation of litigation is an entirely independent and more expansive duty.

This Part addresses these issues first by providing an overview of the scope of the duty to preserve discoverable information and discussing the trigger for that duty. Next, this Part turns to the available remedies and safeguards. Finally, this Part concludes that although some solutions already exist, more drastic action may be necessary to guarantee the authenticity of a medical record produced for litigation.

A. The Scope of the Duty to Preserve Medical Records

The rules of discovery provide that a party has a duty to preserve discoverable information "in the anticipation or con-

---

.com/news/electronic-health-records-pose-several-challenges-as-appeared-in-the-national-law-journal/ [https://perma.cc/QC7J-PATV].

151. *See Electronic Medical & Health Records*, *supra* note 22.

152. This practice is similar to the way in which a cell phone manufacturer provides updates. For example, iPhone users may receive iOS updates that change the way data looks. These updates can cause the system to "crash," resulting in a loss of data in some instances.

153. *See* Zubulake v. UBS Warburg, LLC (*Zubulake IV*), 220 F.R.D. 212, 216 (S.D.N.Y 2003).

154. 42 C.F.R. § 482.24 (2017). The term "Medicare provider" or "Medicaid provider" refers to any provider who treats Medicare or Medicaid patients, regardless of whether the specific plaintiff's or patient's care may be reimbursed by those programs. Notably, there are different preservation obligations under HIPAA (six years) and HITECH (also six years).

duct of litigation."[155] That duty to preserve extends to all relevant information that makes any party's claim or defense more or less probable.[156] Electronic records certainly complicate the duty to preserve in the context of medical negligence suits because every communication or documentation related to a patient's care is "likely to have discoverable information that the disclosing party may use to support its claim or defenses"[157] and thus is "reasonably likely to be requested."[158]

Although no one has ever legitimately disputed that this duty to preserve extends to the legal health record, the legal reproduction of the original record is often incomplete—that is, it omits certain documents and files that are contained within the native EMR.[159] In this way, the common law duty to preserve the medical record in anticipation of litigation is broader than the duty to preserve the medical record under Medicare. Because the preservation duty extends to all potentially relevant and discoverable evidence, the common law duty extends to audio files, video files, images, nursing notes, text messages, and metadata, all of which may not be in the legal health record required to be preserved for Medicare purposes.[160]

Nevertheless, the scopes of the duty to preserve and, subsequently, the duty to produce have been the subject of endless discovery disputes. These discovery disputes largely arise from the confusion concomitant with multiple governing bodies regulating the duty to preserve. Although the FRCP extend the duty to preserve to all potentially discoverable information,[161] the FRCP were not designed with any particular kind of lawsuit in mind. Moreover, the applicable body of federal regulations simply defines the duty to preserve as reaching any information used to make medical decisions during the course of treatment.[162]

---

155. FED. R. CIV. P. 37(e).

156. *See* FED. R. CIV. P. 26(b)(1).

157. *Zubulake IV*, 220 F.R.D. at 218.

158. *Id.* at 217. For the time being, the analysis here sets aside the limitations placed on the scope of discovery by the FRCP proportionality analysis because the duty to preserve extends to any request for discovery. However, because the duty to preserve is framed in terms of probability, it is thus broader than the eventual duty of production.

159. *See supra* Part III (discussing the "Production Problem").

160. *See id.* (discussing what material is contained in the legal health record versus the native file).

161. *See supra* Part III.

162. *See* 42 C.F.R. § 482.24 (2017).

These rules and regulations create ambiguity about *how* a provider is supposed to preserve a patient's record. Providers have a duty under Medicare to preserve medical records in their "original or legally reproduced form,"[163] and HIPAA requires providers to keep and disclose a "designated record set."[164] Because of these regulations, a reasonable provider may mistakenly believe that the duty to preserve extends only to the legal health record. The plaintiff-patient's access to her own records in discovery, however, is not limited to evidence designated *by the defendant-provider* as part of the legal health record. Permitting such a limited view of discovery allows concealment of relevant evidence, which violates the basic tenets of discovery.

The American Bar Association (ABA) guidelines on the duties to preserve and disclose are also lacking in the EMR context, leaving providers and defense lawyers in the dark regarding their legal and ethical obligations. While the scope of the preservation and production duties are quite expansive, the range of applicable guidance is thus very limited.

B. Triggering the Duty to Preserve EMRs

Even though a provider's duty to preserve is quite broad, the scope of that duty is completely meaningless without a clear moment that triggers it. As such, the second major issue is determining at which point a provider is subject to a duty to preserve. The duty to preserve arises when a party reasonably anticipates litigation.[165] At the latest, the duty to preserve arises when a complaint is filed;[166] however, a reasonable person may anticipate litigation long before someone files a claim.[167] After a dramatic accident injures someone, persons involved in those events would likely anticipate litigation from

---

163. *Id.* § 482.24(b)(1).

164. *See Summary*, *supra* note 46, at 12.

165. Zubulake v. UBS Warburg, LLC (*Zubulake IV*), 220 F.R.D. 212, 216 (S.D.N.Y 2003).

166. Jason A. Pill & Derek E. Larsen-Chaney, *Litigating Litigation Holds: A Survey of Common Law Preservation Duty Triggers*, 17 J. TECH. L. & POL'Y 193, 206 (2012).

167. *See* Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) ("The duty to preserve material evidence arises not only during litigation, but also extends to that period before the litigation when a party reasonably should have known that the evidence may be relevant to anticipated litigation.").

the date that the accident occurred, which would trigger the provider's duty to preserve material evidence.[168] Once the duty to preserve attaches to material evidence, a party must "suspend its routine retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."[169]

As a practical matter, the trigger date often will not be an issue because of a statutory duty under Medicare to preserve medical information for at least five years, which in most cases will survive the statute of limitations governing a potential medical negligence claim.[170] The more specific question, then, is when the duty to preserve additional materials in anticipation of litigation is triggered.

In the context of medical negligence suits, a provider should reasonably anticipate that it could be sued at four distinct points in time. Working backwards in time, these instances are: (1) the filing of a lawsuit, (2) internal review, (3) a patient's (or a relative's) grievance with the hospital, and (4) the occurrence of an unexpected, adverse event. The first three of these four events often present easy cases. First, a provider certainly anticipates litigation while it is in the course of litigation. Second, state-sanctioned credentialing committees or internal peer-review boards evaluating practicing physicians may discover that a physician has been operating below the standard of care, has a substance abuse problem, or has some other characteristic that could explain an adverse outcome. Any of these findings would certainly place a hospital or other provider on notice.[171] Third, if a patient informs the provider directly that she is concerned that a course of treatment fell below the standard of care, the reasonable provider may anticipate a lawsuit depending on the nature of the complaint.

The fourth event, and the one most proximate to the injury, is the realization that some adverse medical event should not have occurred; but that realization is not always clear. People die in hospitals, and not every death or complication is

168. *Zubulake IV*, 220 F.R.D. at 206–07.

169. *Id.* at 218.

170. *See* 42 C.F.R. § 482.24(b)(1) (2017) ("Medical records must be retained in their original or legally reproduced form for a period of at least 5 years.").

171. This argument assumes that a prospective plaintiff can offer such proof in light of the peer review privilege, which protects peer review proceedings from discovery. This may come up in cases where a plaintiff offers proof that a treating physician lost privileges at a hospital on some date after peer review.

unexpected. Medical procedures carry risks, and patients should reasonably understand and accept those risks under generally accepted principles of informed consent. Nevertheless, patients expect that reasonable care will be given, and they have reasonable expectations of the risks associated with their plan of care. For instance, patients do not expect to get infections from simple procedures or to suddenly enter septic shock after a routine surgery.

When unexpected, adverse events such as these occur, patients or their loved ones often leave the hospital with questions about what went wrong and look to their providers for answers. A potential litigant may have voiced her concerns and questions directly to the provider. Even without the patient filing a formal grievance, the provider would at least know that the patient is upset and may suspect that the patient might sue if an injury occurred. As such, the duty to preserve evidence may arise as early as the event itself, depending on the nature of the injury. As with the scope of the duty to preserve, however, no authoritative source has provided any meaningful guidance on what triggers the duty to preserve. Consequently, both sides often lose valuable information.

C. Potential Solutions to the Preservation Problem

EMRs present unique preservation issues in electronic discovery because EMRs, unlike emails or customer files, are designed to change.[172] A patient's health information could be updated during the course of litigation, or the EMR software may be updated, which could alter the record to some extent. Providers may be placed in a difficult situation when a record changes during the course of litigation. This situation creates problems of credibility and risks subjecting the provider to a spoliation claim.[173] The malleable nature of EMRs also creates headaches for plaintiffs. A plaintiff who is attempting to authenticate a changing record may have to reconstruct the original record, which expends valuable time and resources. Accordingly, EMRs that lack preservation capabilities are detrimental to both parties and may lead to an unjust result.

---

172. *See Electronic Medical & Health Records*, *supra* note 22.

173. Spoliation, described below, is a tort action against a person who negligently, knowingly, or intentionally destroys discoverable evidence to the detriment of an adverse party.

Because medical records are designed to be changed to reflect up-to-date information, litigants could potentially abuse that changeability to alter the record in their favor. In other words, a doctor or nurse who recognizes a mistake in hindsight could document the care that *should have been* given instead of the care that was *actually* given. Indeed, lawyers must handle an altered record on a regular basis. Some studies estimate that approximately one-half of all records in medical negligence cases have been altered, and approximately one-in-ten records have been fraudulently altered.[174] Apart from subjecting a producing party to an adverse inference, unexplained evidence of alterations raises issues of a provider's credibility—before both a judge and a jury—creating an additional challenge for providers facing illegitimate claims.[175] The ability to authenticate the medical record is crucial to both parties' ability to litigate their claims and to the larger judicial interest in accurate fact-finding. To further those interests, this Section presents several proposals.

1. Proposal A: Require That an Audit Trail Be Automatically Discoverable

Of course, the best time to address the destruction of evidence is before that destruction occurs. An EMR has several functions that help preserve the record, but these functions are not perfect. For example, to authenticate the record, litigants may need access to EMR metadata, which contains data about the data in the EMR.[176] The metadata, or "audit trail," indicates who accessed a record, at what time, and in what way. The example commonly used to explain metadata is an analogy to a Microsoft Word document.[177] When a Word document is

174. Casamassima, *supra* note 108, at 236–37.

175. *See* Hudock & Christ, *supra* note 150 ("As lawyers attempt to establish the authenticity of a dynamically generated electronic document, they often are put in the difficult situation of explaining to opposing counsel, and potentially the trial judge, that an electronic health record is not a static document but rather a living document that is continually changing. Issues are further complicated when one set of medical records data is produced to opposing counsel and a few months later the same set of data is produced again and the data do not match. The failure of a system to produce repeatable, consistent results can turn even the most technologically friendly judge into a skeptic.").

176. *See* Thomas R. McLean, *EMR Metadata Uses and E-Discovery*, 18 ANNALS HEALTH L. 75, 77 (2009).

177. *See id.* at 75–76; *see also, e.g.*, Masor, *supra* note 79, at 252.

created on a computer, the computer indicates the author of the document as well as the date and time the document was created and last modified. Because metadata and audit trails keep track of every edit, they are useful tools to authenticate the record and are thus within the scope of discovery.[178]

EMR metadata can show which computer accessed the record, identify the user who accessed it, indicate when that user accessed it, and sometimes indicate the nature of the change (e.g., an addition or modification).[179] However, an audit trail will not always indicate precisely what changed.[180] For instance, a program may encapsulate a data point in parentheses to indicate a change, but no one—including providers—will be able to see the original value. In these cases, neither courts nor plaintiffs nor providers can determine whether someone fraudulently or legitimately changed the record. Without a more detailed track-changes function, authenticity and credibility issues will continue to plague the courts in medical negligence disputes, despite the relative benefits of the audit trail.

2. Proposal B: Sanctions Should Be a Last Resort, Not the First Instinct

Once information is lost, entirely new questions arise: whether the information lost was valuable, and whether the information lost was intentionally deleted to inhibit discovery.[181] Under the tort of spoliation, any destruction of relevant documents is presumed to be at least negligent and is therefore presumed to be a breach of the duty to preserve.[182] The burden to produce evidence of the non-negligent destruction of records thus shifts to the defendant. As mentioned above, the defendant could show that evidence was destroyed during an update or in the usual course of business.[183] If the defendant fails to

178. Masor, *supra* note 79, at 254.

179. *Id.*

180. *Id.*

181. *See Zubulake IV*, 220 F.R.D. 212, 220–21 (S.D.N.Y 2003).

182. *Id.* at 220 ("Once the duty to preserve attaches, any destruction of documents is, at a minimum, negligent."). The presumption of negligence is intuitive because the duty to preserve turns on reasonable notice, and destruction of evidence in the event of reasonable notice is thus imprudent and sufficient to qualify as a breach.

183. For further discussion on this point, see the introductory paragraphs *supra* in Section IV.C.

overcome that presumption of negligence and the plaintiff demonstrates "that the destroyed evidence would have been favorable" to her case,[184] a court may create an adverse inference that the lost information was unfavorable to the defendant.[185] Further, the court may dismiss the action or enter a default judgment[186] if "necessary to cure the prejudice."[187] As a matter of course, adverse inferences or default judgments are measures administered according to judicial discretion.[188] Consequently, the destruction of evidence that is subject to a duty to preserve, without more, does not guarantee that the adverse party is entitled to an adverse inference or any other remedy.[189]

That said, an adverse inference is a drastic remedy and tends not to be levied against healthcare providers. One way that a provider can avoid an adverse inference from destroyed data is by arguing that the data is not exclusively within the provider's control.[190] An EMR system is, to some degree, within the control of the provider's vendor.[191] Those vendors sometimes issue updates, which can change the organization of the data and could theoretically corrupt it. Because health information is so heavily regulated, however, such instances should

184. *Zubulake IV*, 220 F.R.D. at 221.

185. FED. R. CIV. P. 37(e)(2)(A)–(B).

186. FED. R. CIV. P. 37(e)(2)(C).

187. FED. R. CIV. P. 37(e)(1).

188. *See* Casamissima, *supra* note 108, at 240 ("The inference against the spoliator serves three main functions: (1) accurate factfinding; (2) compensation of the party placed at a disadvantage by the act of spoliation; and (3) punishment of the spoliator.") "Intentional" destruction is traditionally an element of spoliation. However, judicial discretion is normally exercised by interpreting "intent" to mean either an intentional act of destruction (general intent) or an intentional act to deprive or hide information (specific intent). *See, e.g., Zubulake IV*, 220 F.R.D. at 220 (interpreting the "culpable state of mind" as encompassing both the intent to deceive the court and the negligent destruction of material evidence). This distinction can easily be grafted into the EMR discovery context. Depending on the nature of the destruction, a court could apply a more limited remedy (such as an adverse inference) or no remedy at all where the intent existed merely in the act of destruction and the party therefore negligently deprived the court of meaningful discovery. On the other hand, dismissal or default judgment may be appropriate "to cure the prejudice" where a party intentionally hides evidence. FED R. CIV. PRO. 37(e)(1).

189. *See, e.g., Zubulake IV*, 220 F.R.D. at 222.

190. *See, e.g., id.* at 220. Several jurisdictions have specified that "control" for spoliation purposes means "exclusive control." *See, e.g.*, Battocchi v. Wash. Hosp. Ctr., 581 A.2d 759, 766 (D.C. 1990) (malpractice action involving a spoliation issue).

191. Examples of EMR vendors include Epic Systems and Cerner.

be rare. Nonetheless, EMR data is not exclusively within the control of the provider, so the tort of spoliation cannot provide an adequate check on potentially fraudulent changes.

3. Proposal C: Update the Meaningful Use Requirements to Include a Track-Changes Function

In lieu of severe sanctions for altered or insufficient records, authentication and preservation problems can be solved by supplementing the design of EMR systems. Specifically, EMRs should include a clear track-changes function. This feature would not only permit litigants to reconstruct the actual events that took place but also enable litigants and quality assurance personnel to discern which changes were legitimate and which were fraudulent. Providing a clear track-changes functionality similar to the track-changes functionality on Microsoft Word[192] would remedy the Preservation Problem by clearly demarcating which values have been changed, when they were changed, how they were changed, and by whom they were changed.

A track-changes functionality for EMRs would benefit plaintiffs, defendants, and the courts in the aggregate. Where changes to the EMR were appropriate, providers could more easily justify those changes without losing credibility before a judge or jury. Where those changes were fraudulent, a litigant could easily reconstruct the record to reflect the actual care provided and the actual facts known at the time. Thus, a track-changes function would further the judicial interest in accurate factfinding by preventing the destruction of evidence and by preventing any unjustified damage to a provider's credibility. While courts should continue to rely on audit trails to authenticate the record, Congress and CMS could assist the courts and litigants in medical negligence actions by subsidizing the use of EMRs with a track-changes functionality under the meaningful use program.

---

192. As in Microsoft Word, for example, the track-changes function could be hidden while a provider is using the record. An altered value could be indicated by a different color or an asterisk, and the original value would be visible by hovering the cursor over the value. This way, a track-changes function would not fundamentally alter the record while it is being used by providers caring for a patient.

CONCLUSION

As the third-leading cause of death in the United States, medical errors pose a serious threat to the public health. That these harms arise in a place of healing is a bitter irony, and everyone has some interest in reducing the frequency of medical errors. Providers can reduce the frequency of medical errors by improving protocols, developing medical technologies, and educating caregivers. At the same time, courts and legislatures can play a part in helping the victims who fall through the cracks and in protecting providers from unmeritorious claims. This Comment has identified three commonly vexing areas in which courts and legislatures can streamline the EMR discovery process through both short- and long-term solutions.

First, a common point of contention is whether HIPAA implicates the scope of discovery in a medical negligence lawsuit, referred to in this Comment as the Privilege Problem. Courts could clarify that HIPAA (1) does not impose a privilege against a patient attempting to access her own records for the purpose of discovery but (2) may impose a presumptive privilege against the discoverability of other patients' records. Distinguishing between HIPAA disclosures and discovery disclosures in the early stages of a lawsuit can help clarify the scope of discovery without the need for motions practice on the issue.

Second, patients and providers suffer from the Production Problem created by confusion over which form and format of the medical record to produce. While the record exists in many forms, the native record (as it appears on a provider's computer) is the most usable form of the record for all parties involved. Importantly, this native form of the record is discoverable under the FRCP's proportionality factors. Whereas hospitals will have little to no trouble accessing the entire unredacted record during the course of litigation, plaintiffs, physicians, and mid-level providers often struggle to litigate their right of equitable access to that form of the record. Because hospitals, physicians, and patients should be on an equal playing field concerning the availability and usability of information in a medical negligence action, all parties should be able to access that information. While Congress and CMS can facilitate this process by updating the meaningful use requirements, courts can create a rebuttable presumption that the native record is

discoverable and remotely accessible to all parties, subject to limitations set forth in a protective order.

Third, providers and plaintiffs often encounter a Preservation Problem, litigating the authenticity and completeness of the record. Although courts should continue to permit the use of audit trails to authenticate a record, legislatures can streamline authentication litigation by subsidizing a track-changes function in EMR systems.

The stakes in a lawsuit alleging medical negligence are often high, so a readable, usable, and accurate record is crucial to ensure that the loss from an injury occurring within a healthcare institution "lies where it falls."[193] Together, the solutions proposed in this Comment would streamline the discovery process to the benefit of both patients and providers in pursuit of that just result. These solutions would ease the recovery of damages for victims of medical negligence and streamline the imposition of liability on physicians whose negligence caused the injury. At the same time, by expanding access to the medical record for providers and authorizing the use of a readable record for litigation, providers could more effectively defend against unmeritorious claims, thereby protecting their practices and livelihoods from unjustified and potentially unbearable liabilities.

Discovery in a lawsuit alleging medical negligence should be designed for and capable of fair, complete, and accurate fact-finding. Solutions should weigh a provider's practical concerns against a plaintiff's right to her own health information. The proposals presented in this Comment seek to strike that balance, alleviating the strain that medical negligence suits place on the judicial system while promoting a fair and just result. By adopting the solutions advocated by this Comment, courts and legislatures could improve the litigation of medical negligence claims to the benefit of plaintiff-patients, defendant-providers, and the judicial system as a whole.

193. *See* text accompanying note 32 *supra* (discussing the purpose of tort).

UNITED STATES POSTAL SERVICE®

Statement of Ownership, Management, and Circulation (All Periodicals Publications Except Requester Publications)

1. Publication Title	2. Publication Number	3. Filing Date
University of Colorado Law Review	0 0 4 1 - 9 5 1 6	9/20/18
4. Issue Frequency	**5. Number of Issues Published Annually**	**6. Annual Subscription Price**
4 issues within 6 months	four (4)	$45.00

7. Complete Mailing Address of Known Office of Publication *(Not printer)* (Street, city, county, state, and ZIP+4®)

320-C Wolf Law Building
2450 Kittredge Loop Road
Boulder County
Boulder, CO 80309-0401

Contact Person: Jackie Koehn
Telephone (Include area code): 303-492-6145

8. Complete Mailing Address of Headquarters or General Business Office of Publisher *(Not printer)*

320-C Wolf Law Building
2450 Kittredge Loop Road
Boulder County
Boulder, CO 80309-0401

9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor *(Do not leave blank)*

Publisher *(Name and complete mailing address)*

University of Colorado Hannah Regan-Smith, Publisher; Robert McCary, Managing Editor; 2450 Kittredge Loop Drive 320-D, 401 UCB, Boulder, CO 80309-0401

Editor *(Name and complete mailing address)*

Hannah Regan-Smith
University of Colorado Law Review
320D Wolf Law Building
2450 Kittredge Loop Road -401 UCB
Boulder, CO 80309-0401

Managing Editor *(Name and complete mailing address)*

Robert McCary
University of Colorado Law Review
320D Wolf Law Building
2450 Kittredge Loop Road -401 UCB
Boulder, CO 80309-0401

10. Owner *(Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)*

Full Name	Complete Mailing Address
University of Colorado Law School	University of Colorado Law School
	320-D Wolf Law Building
	401 UCB
	Boulder, CO 80309

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box → ☐ None

Full Name	Complete Mailing Address

12. Tax Status *(For completion by nonprofit organizations authorized to mail at nonprofit rates)* *(Check one)*

The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:

☐ Has Not Changed During Preceding 12 Months

☐ Has Changed During Preceding 12 Months *(Publisher must submit explanation of change with this statement)*

13. Publication Title	14. Issue Date for Circulation Data Below
University of Colorado Law Review	Vol. 90, Issue 1-4

15. Extent and Nature of Circulation			Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies *(Net press run)*			221.75	200
b. Paid Circulation *(By Mail and Outside the Mail)*	(1)	Mailed Outside-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	114.25	105
	(2)	Mailed In-County Paid Subscriptions Stated on PS Form 3541 (Include paid distribution above nominal rate, advertiser's proof copies, and exchange copies)	4	4
	(3)	Paid Distribution Outside the Mails Including Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid Distribution Outside USPS®	0	0
	(4)	Paid Distribution by Other Classes of Mail Through the USPS (e.g., First-Class Mail®)	0	0
c. Total Paid Distribution *(Sum of 15b (1), (2), (3), and (4))*			108.75	100
d. Free or Nominal Rate Distribution *(By Mail and Outside the Mail)*	(1)	Free or Nominal Rate Outside-County Copies included on PS Form 3541	5	5
	(2)	Free or Nominal Rate In-County Copies included on PS Form 3541	0	0
	(3)	Free or Nominal Rate Copies Mailed at Other Classes Through the USPS (e.g., First-Class Mail)	0	0
	(4)	Free or Nominal Rate Distribution Outside the Mail (Carriers or other means)	0	0
e. Total Free or Nominal Rate Distribution *(Sum of 15d (1), (2), (3) and (4))*			5	5
f. Total Distribution *(Sum of 15c and 15e)*			113.75	105
g. Copies not Distributed *(See Instructions to Publishers #4 (page #3))*			108	95
h. Total *(Sum of 15f and g)*			221.75	200
i. Percent Paid *(15c divided by 15f times 100)*			100	100

* If you are claiming electronic copies, go to line 16. If you are not claiming electronic copies, skip to line 17.

16. Electronic Copy Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Paid Electronic Copies		
b. Total Paid Print Copies (Line 15c) + Paid Electronic Copies (Line 16a)		
c. Total Print Distribution (Line 16b) + Paid Electronic Copies (Line 16a)		
d. Percent Paid (Both Print & Electronic Copies) (16b divided by 16c × 100)		

☐ I certify that 50% of all my distributed copies (electronic and print) are paid above a nominal price.

17. Publication of Statement of Ownership

☒ If the publication is a general publication, publication of this statement is required. Will be printed in the fifth issue of this publication. ☐ Publication not required.

18. Signature and Title of Editor, Publisher, Business Manager, or Owner	Date
Hannah Regan Smith	9/18/18

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

UNIVERSITY OF COLORADO LAW REVIEW (U.S.P.S. 651-080, ISSN 0041-9516)
Published quarterly by the University of Colorado Law Review,
320-D Wolf Law Building, 401 UCB, Boulder, CO 80309-0401.

Periodicals postage paid at Boulder, Colorado,
and at additional mailing offices.

POSTMASTER: Please send address changes to University of Colorado
Law Review, 320-D Wolf Law Building, 401 UCB,
Boulder, CO 80309-0401.

An association of students, sponsored by the
University of Colorado Law School.

Published as the ROCKY MOUNTAIN LAW REVIEW from 1928 to 1962.

Subscriptions

Current subscription prices: domestic and Canada, $45.00 per volume; foreign, $50.00 per volume; single issues, $25.00. Colorado subscribers must pay sales tax in addition to the purchase price. Contact the Office Manager for the correct payment information before remitting a check.

Subscriptions are entered for an entire volume only and are payable in advance. A check should accompany an order. All subscriptions must be renewed on a yearly basis. Unless a claim for non-receipt of an issue is made within six months after the mailing date, that issue will not be supplied free of charge. Back issues are available.

All subscription correspondence should be addressed to the University of Colorado Law Review, 320-D Wolf Law Building, 401 UCB, Boulder, CO 80309-0401. We may be reached by telephone, 303-492-6145; fax, 303-735-0169; or email, cololrev@colorado.edu. The *Colorado Law Review* web page is located at http://lawreview.colorado.edu.

Manuscripts

The *Colorado Law Review* welcomes the submission of unsolicited manuscripts. The *Colorado Law Review* uses Scholastica, an electronic submission service, which can be reached at https://scholasticahq.com. If you are not affiliated with a university, you may submit your article through Scholastica directly. The *Colorado Law Review* does not accept direct submissions by mail or e-mail. Manuscripts should be double-spaced and no longer than seventy-five pages. Citations should conform to *The Bluebook: A Uniform System of Citation* (20th ed. 2015).

Cite as: 90 U. COLO. L. REV. __ (2019).

THE UNIVERSITY OF COLORADO LAW SCHOOL

FACULTY, 2018–2019

Deans

S. JAMES ANAYA, *Dean and Charles Inglis Thompson Professor of Law.* B.A., University of New Mexico; J.D., Harvard University.

MARK LOEWENSTEIN, *Associate Dean for Curricular Affairs and Monfort Professor of Commercial Law.* A.B., J.D., University of Illinois, Champaign-Urbana.

SARAH KRAKOFF, *Associate Dean for Faculty Affairs & Research and Moses Lasky Professor of Law.* B.A., Yale University; J.D., University of California, Berkeley.

AMY GRIFFIN, *Associate Dean for Instructional Development.* B.A., Boston College; J.D., University of California, Berkeley.

WHITING LEARY, *Senior Assistant Dean for Students.* B.A., Williams College; J.D., University of Colorado.

JENNIFER SULLIVAN, *Senior Assistant Dean for Administration and Program Development.* B.A., Case Western Reserve University; J.D., Duke University.

KRISTINE M. JACKSON, *Assistant Dean for Admissions & Financial Aid.* B.S., University of North Carolina; J.D., George Mason University.

MARCI FULTON, *Assistant Dean for Employer Relations and Outreach.* B.A., J.D., University of Colorado.

TODD ROGERS, *Assistant Dean for Career Development.* B.S., Trinity University; J.D., University of Texas.

FERNANDO GUZMAN III, *Assistant Dean for Diversity, Equity and Inclusive Excellence.* B.S., Santa Clara University; Ph.D., University of Denver.

JESSICA HELZER, *Assistant Dean for Advancement.* B.A., Colorado State University.

Emeritus Faculty

HAROLD H. BRUFF, *Professor Emeritus.* B.A., Williams College; J.D., Harvard University.

EMILY M. CALHOUN, *Professor Emeritus.* B.A., M.A., Texas Tech University; J.D., University of Texas.

JAMES N. CORBRIDGE, JR., *Professor Emeritus.* A.B., Brown University; LL.B., Yale University.

TED J. FIFLIS, *Professor Emeritus.* B.S., Northwestern University; LL.B., Harvard University.

H. PATRICK FURMAN, *Clinical Professor Emeritus.* B.A., J.D., University of Colorado.

WAYNE GAZUR, *Professor Emeritus.* B.S., University of Wyoming; J.D., University of Colorado; LL.M., University of Denver.

DAVID S. HILL, *Professor Emeritus.* B.S., J.D., University of Nebraska.

J. DENNIS HYNES, *Professor Emeritus.* B.A., LL.B., University of Colorado.

HOWARD C. KLEMME, *Professor Emeritus.* B.A., LL.B., University of Colorado; LL.M., Yale University.

ROBERT F. NAGEL, *Professor Emeritus.* B.A., Swarthmore College; J.D., Yale University.

WILLIAM T. PIZZI, *Professor Emeritus.* A.B., Holy Cross College; J.D., Harvard University; M.A., University of Massachusetts.

PETER N. SIMON, *Professor Emeritus.* B.S., M.D., University of Wisconsin; J.D., University of California, Berkeley.

ARTHUR H. TRAVERS, JR., *Professor Emeritus.* B.A., Grinnell College; LL.B., Harvard University.

MICHAEL J. WAGGONER, *Professor Emeritus.* A.B., Stanford University; LL.B. Harvard University.

MARIANNE WESSON, *Professor Emeritus.* A.B., Vassar College; J.D., University of Texas.

CHARLES F. WILKINSON, *Distinguished Professor Emeritus.* B.A., Denison University; LL.B., Stanford University.

Tenured and Tenure-Track Faculty

J. BRAD BERNTHAL, *Associate Professor of Law.* B.A., University of Kansas; J.D., University of Colorado.

FREDERIC BLOOM, *Professor of Law.* B.A., Washington University in St. Louis; J.D., Stanford University.

ALEXIA BRUNET MARKS, *Associate Professor of Law.* B.A., Colgate University; M.S., Ph.D., Purdue University; J.D., Northwestern University.

PAUL F. CAMPOS, *Professor of Law.* A.B., M.A., J.D., University of Michigan.

DEBORAH J. CANTRELL, *Associate Professor of Law and Director of Clinical Programs.* B.A., Smith College; M.A., University of California, Los Angeles; J.D., University of Southern California.

KRISTEN A. CARPENTER, *Council Tree Professor of Law and Director of the American Indian Law Program.* B.A., Dartmouth College; J.D., Harvard University.

MING HSU CHEN, *Associate Professor of Law, Courtesy Appointment in Political Science, Ethnic Studies Faculty Affiliate, and Director of the Immigration Law and Policy Program.* A.B., Harvard University; J.D., New York University; Ph.D., University of California, Berkley.

RICHARD B. COLLINS, *Professor of Law.* B.A., Yale University; LL.B., Harvard University.

JUSTIN DESAUTELS-STEIN, *Associate Professor of Law.* B.A., University of North Carolina, Ashville; J.D., University of North Carolina, Chapel Hill; LL.M., Harvard University.

KRISTELIA GARCÍA, *Associate Professor of Law.* B.A., Columbia University; J.D., Yale University.

ERIC GERDING, *Professor of Law and Wolf-Nichol Fellow.* B.A., Duke University; J.D., Harvard University.

AYA GRUBER, *Professor of Law.* B.A., University of California, Berkeley; J.D., Harvard University.

LAKSHMAN D. GURUSWAMY, *Nicholas Doman Professor of International Environmental Law & International Energy Programs GWC.* LL.B., Sri Lanka; Ph.D., University of Durham, U.K.

JENNIFER S. HENDRICKS, *Professor of Law and Co-Director of the Juvenile & Family Law Program.* B.A., Swarthmore College; J.D., Harvard University.

PETER HUANG, *Professor of Law and DeMuth Chair.* A.B., Princeton University; S.M., Harvard University; J.D., Stanford University; Ph.D., Harvard University.

SHARON JACOBS, *Associate Professor of Law.* B.M., Cleveland Institute of Music; M.M., Julliard/Columbia University Exchange Program; J.D., Harvard University.

MARGOT KAMINSKI, *Associate Professor of Law.* B.A., Harvard University; J.D., Yale University.

CRAIG KONNOTH, *Associate Professor of Law.* B.A., Fordham University; M.Phil., University of Cambridge; J.D., Yale University.

BENJAMIN LEVIN, *Associate Professor of Law.* B.A., Yale University; J.D., Harvard University.

SUZETTE MALVEAUX, *Provost Professor of Civil Rights Law and Director of The Byron R. White Center*, B.A., Harvard University; J.D., New York University.

SCOTT A. MOSS, *Schaden Chair in Experiential Learning and Professor of Law.* B.A., M.A., Stanford University; J.D., Harvard University.

CHRISTOPHER B. MUELLER, *Henry S. Lindsley Professor of Procedure & Advocacy.* A.B., Haverford College; J.D., University of California, Berkeley.

HELEN NORTON, *Professor of Law and Ira C. Rothgerber Chair in Constitutional Law.* B.A., Stanford University; J.D., University of California, Berkeley.

SCOTT R. PEPPET, *Professor of Law and Wolf-Getches Fellow.* B.A., Cornell University; M.S., University of Colorado; J.D., Harvard University.

CAROLYN B. RAMSEY, *Professor of Law.* B.A., University of California, Irvine; M.A., J.D., Stanford University.

PIERRE J. SCHLAG, *University Distinguished Professor and Byron R. White Professor of Law.* B.A., Yale University; J.D., University of California, Los Angeles.

ANDREW SCHWARTZ, *Professor of Law.* Sc.B., Brown University; J.D., Columbia University.

SCOTT SKINNER-THOMPSON, *Associate Professor of Law, Affiliate Faculty for the LGBTQ Studies Program.* B.A., Whitman College; LL.M., J.D., Duke University.

ANNA SPAIN BRADLEY, *Associate Professor of Law, Assistant Vice Provost for Faculty Development and Diversity, and Faculty Director for the LLM and MSL Degree Program.* B.A., Denison University; J.D., Harvard University.

SLOAN SPECK, *Associate Professor of Law.* B.A., Rice University; M.A., J.D., University of Chicago; LL.M., New York University.

MARK SQUILLACE, *Raphael J. Moses Professor of Law.* B.S., Michigan State University; J.D., University of Utah.

HARRY SURDEN, *Associate Professor of Law.* B.A., Cornell University; J.D., Stanford University.

PHILIP J. WEISER, *Hatfield Professor of Law & Telecommunications, Dean Emeritus, and Executive Director of the Silicon Flatirons Center.* B.A., Swarthmore College; J.D., New York University.

AHMED WHITE, *Professor of Law and Nicholas Rosenbaum Professor of Law Chair.* B.A., Southern University and A&M; J.D., Yale University.

Clinical Faculty

VIOLETA CHAPIN, *Clinical Professor of Law.* B.A., Columbia University; J.D., New York University.

ANN ENGLAND, *Clinical Professor of Law.* B.A., University of Michigan; J.D., University of Denver.

CARLA FREDERICKS, *Associate Clinical Professor, Director of the Indian Law Clinic.* B.A., University of Colorado; J.D., Columbia University.

SEAN HELLE, *Associate Clinical Professor and Director of the Getches-Green Natural Resources and Environmental Law Clinic.* B.A., Luther College; J.D., University of Iowa.

BLAKE REID, *Associate Clinical Professor.* B.A., J.D., University of Colorado; LL.M., Georgetown University.

COLENE ROBINSON, *Clinical Professor of Law and Co-Director of the Juvenile & Family Law Center.* B.A., Valparaiso University; J.D., Loyola University School of Law, Chicago.

Legal Writing and Appellate Advocacy Faculty

AMY BAUER, *Legal Writing Professor.* B.A., Duke University; J.D., William & Mary School of Law.

TERESA BRUCE, *Legal Writing Professor.* B.S., Colorado State University; J.D., Cornell University.

MEGAN HALL, *Legal Writing Professor.* B.A., Colorado State University; J.D., University of Colorado.

DEREK H. KIERNAN-JOHNSON, *Legal Writing Professor.* A.B., Princeton University; J.D., University of Michigan.

GABRIELLE M. STAFFORD, *Legal Writing Professor.* B.A., University of Pennsylvania; J.D., Boston University.

TODD M. STAFFORD, *Legal Writing Professor.* B.A., Southern Methodist University; J.D., Duke University.

Law Library Faculty

ERIK BECK, *Digital Services Librarian.* B.A., University of Wisconsin; M.S.I.S., University of Texas.

GEORGIA K. BRISCOE, *Associate Director and Head of Technical Services.* B.S., Washington State University; M.A., University of San Diego; A.M.L.S., University of Michigan.

ROBERT LINZ, *Associate Director and Head of Public Services.* B.A., Wake Forest University; J.D., University of Florida; M.L.I.S., Florida State University.

SUSAN NEVELOW MART, *Director of the Law Library and Associate Professor.* B.A., University of California, Santa Cruz; J.D., University of California, Berkeley; M.L.I.S., San Jose State University.

JOAN POLICASTRI, *Collection Services and Research Librarian.* B.A., M.A., University of Colorado, Denver; M.A., University of Denver; Certificate, Denver Paralegal Institute.

KERRI-ANN ROWE, *Student Services and Outreach Librarian.* B.A., Yale University; J.D. University of Notre Dame.

LISA SCHULTZ, *Instructional Services and Research Librarian.* B.A., J.D., University of Nebraska-Lincoln; M.L.S., University of Missouri-Columbia.

KAREN SELDEN, *Metadata Services Librarian.* B.S., Pennsylvania State University; M.L.S., Simmons College.

JILL STURGEON, *Access Services Librarian.* B.A., Brigham Young University; M.A., Wright State University; J.D., M.L.S., University of Arizona.

JANE E. THOMPSON, *Associate Director of Faculty Services and Research.* B.A., University of Missouri; M.A., M.L.L., J.D., University of Denver.

ABOUT THE CONTRIBUTORS

JAMES GRIMMELMANN, *Listeners' Choices*, is Professor of Law at Cornell Tech and Cornell Law School. He studies how laws regulating software affect freedom, wealth, and power. As a lawyer and technologist, he tries to help these two groups understand each other by writing about digital copyright, search engines, social networks, online governance, and other topics in computer and Internet law. He is the author of the casebook *Internet Law: Cases and Problems*, now in its eighth edition, and of over fifty scholarly articles and essays.

BURT NEUBORNE, *Limiting the Right to Buy Silence*, is the Norman Dorsen Professor of Civil Liberties and founding Legal Director Emeritus of the Brennan Center for Justice at the New York University Law School. For more than fifty years, he has been one of the nation's foremost civil liberties lawyers, serving as the National Legal Director of the American Civil Liberties Union (ACLU) from 1981–86, Special Counsel to the NOW Legal Defense and Education Fund from 1990–1996, and as a member of the New York City Human Rights Commission from 1988–92. He has argued numerous U.S. Supreme Court cases and has litigated hundreds of important constitutional cases in the state and federal courts. He challenged the constitutionality of the Vietnam War, pioneered the flag burning cases, worked on the Pentagon Papers case, worked with Justice Ruth Bader Ginsburg when she headed the ACLU Womens Rights Project, anchored the ACLU's legal program during the Reagan years, and defended the Legal Services program against unconstitutional attacks. He is the author of four books and over twenty law review articles on diverse areas of constitutional law and procedure.

HELEN NORTON, *Powerful Speakers and Their Listeners*, is the Ira C. Rothgerber, Jr. Chair in Constitutional Law at the University of Colorado Law School. Her scholarly and teaching interests include constitutional law, civil rights, and employment discrimination law. She served as leader of President-elect Obama's transition team charged with reviewing the Equal Employment Opportunity Commission in 2008, and is frequently invited to testify before Congress and federal agencies

on civil rights law and policy issues. Before entering academia, Professor Norton served as Deputy Assistant Attorney General for Civil Rights at the U.S. Department of Justice, and as Director of Legal and Public Policy at the National Partnership for Women & Families.

DEREK E. BAMBAUER, *The MacGuffin and the Net*, is a Professor of Law at the University of Arizona, where he teaches Internet law and intellectual property. His research focuses on Internet censorship, cybersecurity, and intellectual property. He has also written technical articles on data recovery and fault tolerance, and on deployment of software upgrades. A former principal systems engineer at Lotus Development Corporation (part of IBM), Professor Bambauer spent two years as a Research Fellow at the Berkman Center for Internet & Society at Harvard Law School. At the Berkman Center, he was a member of the OpenNet Initiative, an academic consortium that tests and studies Internet censorship in countries such as China, Iran, and Vietnam. He is one of the authors of *Info/Law*, a popular blog that addresses Internet law, intellectual property, and information law. He holds a Bachelor of Arts degree from Harvard College and a Juris Doctor from Harvard Law School.

RONNELL ANDERSEN JONES, *Press Speakers and the First Amendment Rights of Listeners*, is the Lee E. Teitelbaum Endowed Professor of Law at the University of Utah S.J. Quinney College of Law. A former newspaper reporter and editor, Professor Jones teaches, researches, and writes on legal issues affecting the press and on the intersection between the media and the courts, with a particular focus on the United States Supreme Court. Her work on press issues has appeared in numerous top journals, including the Michigan Law Review, Minnesota Law Review, UCLA Law Review, and Harvard Law Review Forum. Professor Jones graduated first in her law school class, and clerked for the Honorable William A. Fletcher on the Ninth Circuit Court of Appeals and for Justice Sandra Day O'Connor on the U.S. Supreme Court. Prior to entering academia, she was an attorney in the appellate division of Jones Day, where her work focused on Supreme Court litigation and included major constitutional and First Amendment cases.

GREGORY P. MAGARIAN, *When Audiences Object*, is a Professor of Law at the Washington University Law School, where he is a well-known expert in free speech, the law of politics, and law and religion. He has written about a variety of topics in constitutional law, including free speech theory and doctrine, media regulation, regulation of political parties, the relationship between church and state, and substantive due process. A frequent presenter at conferences in the United States and abroad, he has published his scholarship widely in various law reviews. Before becoming a law professor, he clerked for U.S. Supreme Court Justice John Paul Stevens, as well as for the Honorable Louis Oberdorfer, U.S. District Court for the District of Columbia. Professor Magarian also practiced law for five years with the Washington, D.C. firm of Jenner & Block as a litigation associate.

ALEXANDER TSESIS, *Data Subjects' Privacy Rights*, is the Raymond & Mary Simon Chair in Constitutional Law and Professor of Law at the Loyola University, Chicago, School of Law, where he teaches Constitutional Law, First Amendment, Civil Procedure, and seminars devoted to civil rights issues and constitutional interpretation. His articles have appeared in many law reviews, including the Columbia Law Review, Cornell Law Review, Minnesota Law Review, Northwestern University Law Review, and Texas Law Review. His books include *Constitutional Ethos*; *For Liberty and Equality: The Life and Times of the Declaration of Independence*; *We Shall Overcome: A History of Civil Rights and the Law*; *The Thirteenth Amendment and American Freedom: A Legal History*; and *Destructive Messages: How Hate Speech Paves the Way for Harmful Social Movements.*

FELIX T. WU, *Commercial Speech Protection as Consumer Protection*, is a Professor of Law at the Benjamin N. Cardozo School of Law and Faculty Director of the Cardozo Data Law Initiative. His doctorate studies in computer science are foundational to his information law scholarship, which spans freedom of speech, privacy law, and intellectual property law. He has written about the limits of online intermediary immunity, on understanding the role of data de-identification in law, and on the relationship between data privacy and theories of

free expression. Professor Wu received his A.B., *summa cum laude*, in computer science from Harvard University, and both his Ph.D. in computer science and J.D. from the University of California at Berkeley. He clerked for Judge Sandra L. Lynch of the U.S. Court of Appeals for the First Circuit.

JUDGE CARLOS F. LUCERO, *A Constitutional Call to Arms*, is a judge for the United States Court of Appeals for the Tenth Circuit. He was appointed in 1995 by President Clinton. Judge Lucero is from the San Luis Valley in Colorado. He received his undergraduate degree from Adams State University and his law degree from George Washington University Law School. Following law school, Judge Lucero clerked for Judge William E. Doyle of the U.S. District Court for the District of Colorado and then went into private practice in Alamosa, Colorado. Judge Lucero served as the president of the Colorado Bar Association from 1977 to 1978. He has received the Professional Service Award of the Colorado Hispanic Bar Association, Professional Service Award of the League of United Latin American Citizens, the Distinguished Alumnus Award from George Washington University, and the National Jurist of the Year Award from the Hispanic National Bar Association. He is a fellow of the American College of Trial Lawyers, International Academy of Trial Lawyers, International Society of Barristers, American Bar Foundation, and the Colorado Bar Foundation. Judge Lucero is also an honorary member of the University of Colorado Law School Order of the Coif.