Mitigating the E-Discovery Sideshow: Health Care Employer's Guide to Managing E-Discovery Before and During Litigation

Martine Wells*
Hannah M. Caplan
Brownstein Hyatt Farber Schreck LLP
Denver, CO

Employment litigation in today's increasingly digitized health care workplace requires fluency and competency to effectively and efficiently manage discovery of electronically stored information (ESI) or E-Discovery.[1] Health care employers face particular E-Discovery challenges from the moment that they are on notice of potential litigation given the high volume of data, vast number of custodians, and numerous ESI sources that exist and continue to proliferate in that setting. Proactive efforts to understand and manage a facility's digital footprint, and all the myriad sources of data, can help mitigate these challenges. And, anticipating the E-Discovery hurdles that typically arise in employment litigation can prevent stumbling into E-Discovery minefields that can derail a case and disrupt a facility. Likewise, harnessing a facility's ESI early in a case can create an offensive advantage to move the needle in litigation.

Proactive E-Discovery Measures to Undertake Now

There are several steps that heath care employers should take now and on an ongoing basis to prepare the facility for an efficient and defensible E-Discovery process, including:

- Know all potential sources of ESI, including email, servers, local and hard drives, PSTs, mobile devices, pagers, movement trackers, software programs (e.g., Meditech, electronic medical records, HRIS programs, timekeeping systems, etc.), third-party vendor-managed sources, voicemail, non-facility devices (e.g., personal computers and mobile devices that can access and store facility data), video, cloud, backups, enterprise sources, local sources, hardware and other removable storage devices, and other alternative data sources (e.g., messaging systems, Slack, security badge systems, timeclocks, phone systems, movement trackers, fingerprint devices, etc.).
- For each source, identify the timeframe of use, retention polices, storage method and location, persons most knowledgeable about the system, preservation nuances for the system, how easy/hard is it to collect the data, and whether the data can be collected enterprise-wide or custodian-by-custodian.
- Be aware of nontraditional sources of data, including movement and activity trackers (e.g., Fit Bits), appliances with time and other stamps, BYOD (bring your own device), and COPE (co-owned/personally enabled) devices that contain unique facility data that is not fully synced with the facility's system.
- Develop broad relationships with facility resources from IT and legal, outside counsel, and a trusted and repeatedly used vendor to manage and strategize regarding consistent retention, collection, review, and production practices to increase efficiency and the ability to effectively harness the data for use in the litigation. These established relationships will help ensure that E-Discovery processes and retention policies are forensically sound and defensible, and if certain custodians are frequently identified, it is highly recommended to store data with a vendor that can "reuse" the data for other litigation.
- Do not forget about physical documents, which are often overlooked in this E-Discovery environment, but still used, stored, and relevant.

Immediate Steps to Preserve and Collect E-Discovery Materials Once a Claim Is Asserted

Litigation Hold Notices Must Account for ESI

Once a facility reasonably anticipates employment litigation, including at the administrative charge phase, it has a duty to promptly take "reasonable steps" to preserve ESI.[2] A carefully crafted litigation hold notice (Notice) is the first line of defense. The Notice should explicitly set forth the information that is relevant, discoverable, and proportional to the needs of the case;[3] ESI and physical documents covered; affected custodians; timeframes at issue; and the expectation around each source (e.g., make a copy, stop automatic deletion, set aside and notify IT to collect, etc.).

Specifically, identifying the "right" custodians is an integral component of an effective Notice. These custodians should be instructed to consider the specific sources (as listed above) that *they* have access to that could contain relevant ESI, in addition to hard-copy documents and their own personal devices used to access work data.

To the extent enterprise systems are implicated, the Notice should instruct IT to preserve any electronic or software systems, such as payroll, timekeeping, personnel records, and scheduling programs. Additionally, any surveillance video that could potentially capture employee misconduct or tardiness should be preserved.[4] Finally, legal and IT should ensure that automatic deletion is suspended and backups are performed as appropriate.

This process is fluid. Notices should be regularly updated, adding and deleting custodians and ESI sources/parameters as appropriate, and should be audited by outside counsel on a quarterly basis to ensure recipients know of and are following the hold. To the extent multiple copies of the same data are discovered, consider whether all sources must be preserved or if one is sufficient and document the reasoning behind that decision.

Because Notices are generally protected by the attorney-client privilege and/or work product doctrine (absent spoliation or another problem with the process),[5] counsel should carefully consider which custodians should receive hold notices. For example, to the extent non-exempt workers at a facility only have access to email, certain servers, and other work-issued mobile devices, it is likely that a Notice need not be issued to the individual custodian; rather, so long as the custodian is listed on the enterprise-wide IT notice and the data is preserved, that should be sufficient.

Best Practices for ESI Collection of ESI

Naturally, health care employees focus on patient care, and not ESI organization. Nonetheless, health care employers must ensure that all potentially relevant ESI is collected at the inception of a claim. Depending upon the size of the claim, a third-party E-Discovery vendor can be tremendously helpful to the dual objectives of complying with E-Discovery preservation efforts and minimizing disruption to operations. With patient care at the forefront of their minds, health care employees may conduct only cursory searches of their electronic devices, and may not even know all of the places ESI could be hiding. An E-Discovery vendor is able to quickly identify locations of potentially relevant ESI and efficiently collect ESI in its native format.[6]

Regardless of whether an E-Discovery vendor is utilized, custodians should be instructed to work with the facility's IT support to extract emails and data from old and new computers, as well as other electronic systems. It is also important to clarify in the Notice that documents must be preserved in all forms, and if a document exists in paper and electronically, both should be preserved. A paper copy may include handwritten notes that the electronic copy lacks, for instance. Custodians also should be instructed to collect potentially relevant documents on an ongoing basis; for those who frequently use email, a helpful suggestion is to create a file in the email exchange and simply copy emails related to the claim to that folder to be collected in the future. In addition, potentially relevant ESI must be maintained after it is reviewed for relevant or responsive information, as the court may later require a different or more narrowly tailored search through the ESI.[7]

Critically, although E-Discovery can be helpful, the facility's attorney(s) remains ultimately responsible for the discovery process and competent representation.[8]

Managing E-Discovery During an Employment Lawsuit

Avoid Inadvertent Disclosure of Protected Health Information and Other Protected Information

Even in the context of an employment lawsuit, health care employers must remain diligent to safeguard protected health information (PHI) of employees and patients. The Health Insurance Portability and Accountability Act (HIPAA) bars health care employers from disclosing PHI except as permitted or required by the HIPAA regulations.[9] In all cases, health care employers also must carefully review documents that may implicate otherwise protected materials. Specifically, teams should analyze discoverable material for information that may be subject to medical, legal, professional review, and/or quality assurance privileges, as well as confidential credentialing and licensure issues to prevent inadvertent disclosure, breach, and/or waiver of these important privileges and immunities.[10]

It is not uncommon for PHI to appear in documents related to an employment claim, thereby implicating HIPAA. For example, plaintiffs typically request detailed personnel information of similarly situated employees, including information related to accommodations and medical leaves. Unlike the mere fact of leave or accommodation, an employer may have legitimate grounds to object to disclosure of the PHI (including the reason for leave or accommodation) of an employee not party to the lawsuit. Similarly, employee personnel files may contain PHI of the facility's patients, most often in relation to a disciplinary action or commendation related to patient care.

Fundamentally, the nature of a health care facility results in the possibility that PHI could be anywhere, including in personnel files, and health care employers must bear this in mind when responding to discovery requests. Within complex document management systems, there is no specific word or phrase that can be searched to ensure PHI is not inadvertently disclosed; one cannot search for a patient's name whom one does not know exists in a document. Therefore, manual examination of all documents that could potentially contain PHI is critical, notwithstanding the impressive software available for review of electronic documents in discovery. Utilize contract reviewers, or possibly technology-assisted-review, as necessary.

Awareness of the Potential Risks and Benefits of Metadata

Even if not apparent from the face of the document, ESI may contain "metadata," which hides beneath the surface of ESI and can reveal information such as authors, revisions (including the exact timing of revisions), and the location of where the documents were housed within a system. Understanding this "data about data" is essential for health care employers to avoid inadvertently producing PHI or privileged information. For example, consider an employee disciplined for unprofessional conduct toward a patient. If that disciplinary action was drafted in Microsoft Word, it may have originally contained the full name of the patient, before a prudent supervisor thought to remove it. However, the prior version—containing the patient's name—may be apparent in the document's metadata.

Nonetheless, metadata should not be viewed only as a secret carrier of privileged or protected data; consider whether metadata may *help* your case. To illustrate, if the timing of the decision to discipline or terminate an employee is at issue, the original date and content of a Word document documenting that decision may win the case and show that the employee's later protected activity had no bearing on the decision.

Given the considerable potential risks and benefits associated with metadata, health care employers should work with their IT department and a trusted E-Discovery vendor to scan all potentially relevant documents for metadata. Additionally, by considering the potential impact of metadata on a particular claim, the health care employer will better structure the E-Discovery plan, addressed below, to specify the format of production and perhaps excluding or limiting metadata production, among other key limitations and delineations. The decision whether to produce documents in native format (rather than converting Word, Excel, and similar "living" documents to PDF) may change the course of the case.

Proactive and Early Use of E-Discovery Plans in Federal Court

The 2015 amendments to the Federal Rules of Civil Procedure addressed a variety of E-Discovery issues relating to: (1) scope of discovery (prioritizing proportionality[11] and admissibility at trial is no longer a factor), (2) discovery objections (objections must now be stated with specificity, and state whether responsive information is being withheld on the basis of an objection and when a production will begin/end), and (3) indicating that E-Discovery plans are preferable.

We recommend using E-Discovery plans[12] early and often as a tool to launch discussions with opposing counsel at or before the Fed. R. Civ. P. 26(f) conference, while fashioning the scheduling order, and throughout discovery to help frame the contours of the preservation, collection, search, processing, and production obligations and methods that will be used in the case (the burden of which primarily falls to the employer). This plan is critical to support later arguments that, for example, discovery methods utilized have been sufficient, agreed upon, and further endeavors would result in a disproportionate effort and expenditure. This will also help generate an E-Discovery budget for internal use in the case (anticipating what discovery will be needed and the contours of how it will be accomplished).

Martine Wells,* *a shareholder with the Denver-based firm Brownstein Hyatt Farber Schreck LLP, specializes in representing and counseling health care clients to mitigate risk before and during litigation, with a particular focus on wage and hour issues, class/collective actions, and E-Discovery.* ***Hannah Caplan,* *a senior associate with the Denver-based firm Brownstein Hyatt Farber Schreck LLP, specializes in labor and employment litigation, and has counseled health care clients through several iterations of E-Discovery preservation, collection, review, and production.*

---

1 Model Rule of Prof'l Conduct R. 1.1, cmt. 8 (an attorney must keep abreast of "benefits and risks associated with relevant technology" in the practice of law).

2 Fed. R. Civ. P. 37(e) and Advisory Committee Notes to 2015 Amendments; *see also* applicable state rules of civil procedure; *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (preservation duty arises when party has notice or should have known that evidence is relevant to litigation).

3 Fed. R. Civ. P. 26(b)(1), (2)(B).

4 *See, e.g., Loyd v. Saint Joseph Mercy Oakland,* 766 F.3d 580, 587 (6th Cir. 2014) (in response to former hospital employee's motion to compel surveillance footage to counter the grounds for her termination, the hospital could not produce the video because it had been overwritten per hospital policy; the court held that former employee may be entitled to a jury instruction drawing an adverse inference from the hospital's failure to preserve the video).

5 *See, e.g., Gibson v. Ford Motor Co.*, 510 F. Supp. 2d 1116, 1123 (N.D. Ga. 2007).

6 *See* Fed. R. Civ. P. 34(b)(2)(E)(ii) ("If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.").

7 *Novak v. Somerset Hosp.*, No. 3:07cv3042010 (W.D. Pa. Apr. 22, 2010) (holding that "[a]ccess to [hospital] defendants' communications is essential to completing full discovery," and the hospital's initial search terms were "too restrictive").

8 *See* American Bar Association Formal Op. 08-451.

9 45 C.F.R. § 164.502(a).

10 *See, e.g.*, Healthcare Quality Improvement Act of 1986, 42 U.S.C. § 11101; *In re The Colo. Med. Bd.*, 333 P.3d 70 (Colo. 2014).

11 *See, e.g., Wagoner v. Lewis Gale Med. Ctr.*, LLC, No. 7:15cv570 (W.D. Va. July 13, 2016).

12 *See, e.g.*, Initial Discovery Protocols for FLSA Cases Not Pleaded as Collective Actions (Jan. 2018).