

THE HEALTH LAWYER

IN THIS ISSUE

Electronic Discovery and Healthcare Litigation: Government Influence on Conversion to Electronic Health Records, and How It Has and Will Continue to Impact the Discovery Process.... 1

Tobacco Regulation in the United States: New Opportunities and Challenges 13

The Usefulness of Non-Linear Thinking: Conceptual Analysis Tools and An Opportunity to Develop Electronic Health Information Privacy Law 18

Discharging False Claims Liability in Bankruptcy, Section 1141(d)(6)(A) of the Bankruptcy Code: An Incentive to Settle FCA Cases? 40

Health Plans 2011: Healthcare Reform Begins 47



ELECTRONIC DISCOVERY AND HEALTHCARE LITIGATION: GOVERNMENT INFLUENCE ON CONVERSION TO ELECTRONIC HEALTH RECORDS, AND HOW IT HAS AND WILL CONTINUE TO IMPACT THE DISCOVERY PROCESS

Anna M. Bryan, Esq.
Debra A. Weinrich, Esq.
Edward F. Beitz, Esq.

White and Williams LLP
Philadelphia, PA

Introduction

For attorneys and many other professionals working in the electronic age, computers and PDAs are the dominant means of creating, exchanging and storing information. Computer-based information technology has become commonplace, and it is increasingly rare to see pen put to paper in the workplace. In fact, a study conducted at the University of California at Berkeley back in 2003 found that, even then, only 0.01 percent of newly created information was stored in paper format, with the remainder being stored in electronic formats.¹ A more recent study, performed in 2009, found that digitally-stored data now totals 487 billion gigabytes world wide – the equivalent of 19 billion fully-loaded Blu-ray DVDs.² The study estimated that these existing gigabytes of digital content would double in a mere 18 months, and every 18 months thereafter.³

Just as it has changed the practice of law in so many respects, the digital revolution has had a significant impact on the practice of medicine. Yet, for all the advances computer science has contributed to medical science, the healthcare industry remains relatively behind the digital curve when it comes to creating, exchanging and storing patient health information. According to a survey performed by the National Center for Health Statistics in 2008 and 2009, more than 50 percent of physicians were not utilizing any form of electronic health records.⁴ Only 6 percent of physicians were using a “fully functional” electronic health record system.⁵ Over the next five years, this undoubtedly will change.

In addition to implementing new HIPAA rules governing security and privacy, the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) of 2009 (part of the larger Stimulus Act) was intended to hasten the nationwide development of electronic health record (“EHR”) technology. Through the HITECH Act, the government has allocated significant spending in the form of incentives and funding for

continued on page 3

Electronic Discovery and Healthcare Litigation

continued from page 1

medical providers who make “meaningful use” of EHRs. While the federal objectives of a quick and seamless exchange of health information and overall improvement in care quality are certainly laudable, the newly proposed criteria by the federal government will create new obstacles and issues for healthcare attorneys, particularly during the discovery process.

For many litigators, the term “e-discovery” already seems like a well worn concept that has been addressed hundreds of times by various specialists in a myriad of disciplines. However, because many healthcare institutions and physicians have not converted to electronic medical records systems, they, and their counsel, have not yet been faced with responding to an extensive request for electronically stored information. This too will change, given the federal government’s intent to practically mandate provider conversion to an electronic health record format. Accordingly, healthcare attorneys need to be familiar with frequent changes in discovery rules, new case law, and the resulting obligations they impose, not only on their clients, but also on the attorneys themselves. Ultimately, they must realize that the discovery process has become much more difficult and costly, and the landscape is wrought with pitfalls. Understanding the elements of electronic data storage, nuances in client software programs, data collection and storage systems and related policies is crucial to providing appropriate legal counsel.

This article will address the “meaningful use” requirements for developing EHR systems that were proposed by the federal government on December 30, 2009, as well as their impact on the attorneys who must respond to requests for the enormous amount of electronic data that will be created as a result.

Electronically Stored Information

What is electronically stored information (“ESI”)? The simple, common sense answer is “any information stored in an electronic format.”⁶ This sounds very basic. However, that extraordinarily broad definition encompasses an almost incomprehensible glut of data in a healthcare litigation setting. For an attorney who is seeking discovery, such a broad definition is wonderful, as a request for this information could ultimately result in the production of a gold mine of data never before available in litigation. Conversely, the recipient of a subpoena for “all electronically stored information,” often must fight the desire to hide his or her head in the sand rather than face the tremendously daunting task of gathering and reviewing the large amount of potentially responsive data.

ESI is not limited to emails, reports and other documents created by a computer or other electronic device. To the contrary, it also encompasses something called “metadata.” According to the Oxford dictionary, metadata is a “set of data that describes and gives information about other data.”⁷ It has been defined in the federal courts as information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted, including data demographics such as size, location, storage requirements and media information.⁸ Metadata is particularly important in a litigation context. For instance, it firmly establishes who, what and when a document or entry in a document was created or modified. Generally, every action taken on a computer system (e.g., inputted data, deletions, and corrections) leaves a trail. Some of those trails are easily accessible, while others require forensic examination and are not routinely addressed in litigation. Importantly,

the new proposed criteria for EHRs, which will be discussed below, require that electronic health information technology “[r]ecord actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, deleted, or printed; and an indication of which action(s) occurred must also be recorded.”⁹

Many litigators have become accustomed to dealing with requests for emails and electronically created documents. Requests for the metadata associated with those documents are increasingly becoming the subject of motion practice. This has not been yet become a widespread concern in the medical malpractice context, but it likely will in the near future. For example, improper alterations to paper medical records and charts do occur, and often become the subject of motion practice. Proving an improper alteration to a paper medical chart can require complex analysis of the records themselves, often by a handwriting expert or forensic analysis of the ink on the page. On one hand, the conversion to EHRs simplifies proving if and when an alteration was made, and who made it, because the data is entered directly into the computer which tracks such information. Yet, there are still situations where an electronic system does not alleviate all issues concerning record alteration.

For example, when a hospital utilizes handwritten progress notes (as the majority still do) in combination with an EHR system, those progress notes are usually scanned into a computer system. The progress notes themselves may then be destroyed. In such a case, forensic ink analysis is no longer a possibility. Direct entry of information into a computer will eliminate much of the ambiguity about precisely when something was charted by a practitioner. Of course,

continued on page 4

Electronic Discovery and Healthcare Litigation

continued from page 3

electronically tracking health record access is not always perfect. Some existing EHR systems currently access documents, such as a radiology report, but fail to capture whether that same user viewed the related radiology images hyperlinked to the documents. Much depends on the specific configurations in the software. Even if two healthcare systems purchase and utilize the same "brand" of EHR software, purchasers usually have the package customized to their particular institution. Accordingly, the complexities and nuances of connectivity and tracking capabilities at various healthcare institutions will vary, another reason why attorneys should familiarize themselves with their client's systems.

In the context of litigation and discovery practice, sophisticated businesses, corporations and other like parties usually have numerous different sources of stored electronic information. While an individual may have only a few (such as a personal computer, a PDA, and a cell phone), a healthcare institution, such as a hospital, can have a large number of electronic storage sites. There are servers and computers with different programs and access for medical records, radiology records, human resource information, billing information, emails, garage access cards, closed or locked unit access card systems and "intranets." This only scratches the surface. Hospitals also have a large number of employees who themselves utilize cell phones and PDAs which store electronic data.

While electronic data sources are not necessarily part of, or even directly related to, an individual's health record, they may be pertinent in various forms of healthcare litigation. All electronic data sources must be considered to hold potentially relevant, discoverable information. Consequently, even if a party plans on

objecting to a particular discovery request, that party still must consider and evaluate electronic sources of information to determine if it is relevant, responsive to a specific request, or protected by some privilege.

Importantly, ESI and the associated metadata should not necessarily be a source of anxiety. It certainly may be advantageous to be able to prove the exact time a document was created, which can be an issue with paper records when the date and time are omitted due to human error. It likewise may be helpful to know exactly when a doctor swiped his or her identification card in order to gain access to a closed hospital unit. ESI should be carefully reviewed not only because it may be responsive to a discovery request; it may also hold information critical to winning a case.

Electronic Health Records

What is an EHR? The question can be answered simply with the following: a healthcare record that is kept in an electronic format on a computer, as opposed to a paper chart. Another definition for EHR, provided by the National Alliance for Health Information Technology, is "the aggregate electronic record of health-related information on an individual that is created and gathered cumulatively across more than one health care organization and is managed and consulted by licensed clinicians and staff involved in the individual's health and care."¹⁰ By that definition, an EHR is not simply one electronic document containing a patient's health information (medical history, complaints, diagnoses, etc.), but rather it is a collection of all such documents accumulated from multiple office visits and hospitalizations over time.

For attorneys advising their healthcare clients in developing these systems,

helping clients reach compliance for incentive funds, or responding to a discovery request for a patient's records, it is worth noting that the statutory definition of "Qualified Electronic Health Record," as it has been amended by the Public Health Service Act ("PHSA").¹¹ Under the PSHA, a Qualified EHR has defined an electronic record of health-related information on an individual that includes patient demographic and clinical health information, such as medical history and problem lists. Further, a Qualified EHR must have the capacity to provide clinical decision support, allow for electronic entry of physician orders, capture and query information relevant to healthcare quality, and exchange electronic health information with, and integrate such information from other sources.¹²

Even from this short description, it is clear that the future of medicine will look a lot different from the paper charts of old. Of course, some healthcare systems, hospitals and practice groups already have these systems in place, while others are using a hybrid of paper and electronic records. The challenge for those institutions will be to make the necessary changes and upgrades if their existing systems are not compliant under the new federal framework. Likewise, healthcare attorneys who already are accustomed to producing electronic medical records will also have to evolve with the changing times. For example, one of the many requirements for compliant, "meaningful use" of EHR (which will be discussed in more detail below) is that patients must be able to obtain and view a copy of their medical records *in an electronic format*. As this capability becomes common place, it is hard to imagine that thousands of pages of "printout" from an EHR will be viewed as an acceptable or practical discovery method.¹³

In the past, producing certain audit trails and timelines may have proven too burdensome to sustain a motion to compel such information. However, given the proposed requirements for EHR systems, providers and hospitals will have a more difficult time arguing that a given request is too onerous, unless it relates to forensic evaluation and/or production of backup tapes. The new proposed requirements for EHR systems include the ability to track user actions related to the entry of patient information. This includes the date, time, patient identification, and user identification pertaining to when electronic health information is created, modified, deleted, or printed; an indication of which actions(s) occurred must also be recorded.¹⁴ Plaintiff's attorneys familiar with the regulations will be able to argue that such an audit trail or record log should exist and should be accessible by a provider's information technology team.

Assuming the proposed requirements are ultimately incorporated into the final regulations, a hospital will be able to produce a list of every physician or other personnel who accessed a record, as well as all of the electronic alerts given to a provider in the course of treatment. Attorneys experienced with EHR systems know all too well that if someone is accessing a medical record, there had better be a reason. This is true not only in relation to HIPAA's privacy rule, but also in relation to discovery in a healthcare case. For instance, opening a patient's medical record, which is tracked by an EHR system, opens physicians, nurses and others up to, at a minimum, the need to provide deposition testimony. The bottom line, when accessing an electronic record, is to always err on the side of caution, and assume this information will be discoverable.

In a profession where procrastination can be one's downfall, healthcare attorneys would be wise to begin educating themselves about a client's EHR

system when it is implemented. While it is clear these changes are not going to happen overnight, they are coming, and sooner than may have been expected. Given the complexities and nuances of each and every EHR system, healthcare attorneys should get up to speed as soon as possible.

Accelerating The Trend Towards Electronic Health Record Systems

The Medicare and Medicaid reimbursement incentives for "meaningful" users of EHR, mentioned above, will begin in January of 2011 for eligible professionals and eligible hospitals. While the program will begin as purely incentive-based for those who choose to develop and implement EHR systems, beginning in 2015 Medicare payment adjustments will be imposed on professionals who are not meaningful EHR users.¹⁵ The initial incentive payments are not insignificant; equal to 75 percent of Medicare's allowable charges for covered services furnished by the eligible professional in a year, up to \$18,000 in the first year.¹⁶ The amount of incentive payments for eligible hospitals is variable, depending on the number of discharges for each eligible hospital in a given year, the estimated percentage of inpatient bed-days for Medicare fee-for-service and/or managed care patients, and charity care provided by the hospital. These variables are applied to a base starting payment of \$2 million in the first year, and the payments are decreased over four years, with no further payments in the fourth year.¹⁷

Medicare will provide no payments for "meaningful" EHR use after 2016, which reflects the Act's intended purpose to jumpstart the nationwide conversion to EHR. With regard to the payment adjustments (i.e., penalties) on those eligible professionals not making meaningful use of EHR in 2015, reimbursement amounts for covered services will be reduced by

an increasing percentage each year.¹⁸ Hospitals not making meaningful use of EHR by 2015 will also suffer adjustments in the form of a reduction of amounts it would be normally receive to account for inflation.¹⁹

On December 30, 2009, both the Centers for Medicare and Medicare Services ("CMS") and the Office of the National Coordinator for Health Information Technology ("ONC") issued proposed rules and regulations intending to "lay a foundation for improving quality, efficiency and safety through meaningful use of certified electronic health record (EHR) technology."²⁰ An Interim Final Rule issued by ONC on December 30, 2009 (and published in the Code of Federal Regulations on January 13, 2010) also sets initial standards, implementation specifications, and certification criteria for EHR technology, and has provided a proposed set of criteria for "meaningful use."

The Requirements and Capabilities for Meaningful Use of Electronic Health Record Systems

The full set of criteria for Stage I "meaningful use" proposed by CMS is set forth in the Interim Final Rule, which can be downloaded in PDF format from CMS.²¹ The focus of the Stage 1 criteria for "meaningful use" is on electronically capturing health information in a coded format, using that information to track key clinical conditions, communicating that information for care coordination purposes, and initiating the reporting of clinical quality measures and public health information.²² Already, and for any attorney who has received a request for "all metadata," the mind starts to boggle.

The recently proposed CMS rule offers a phased implementation process of meaningful use criteria, a seemingly pragmatic approach to implementing EHR technologies. The Stage I goals

continued on page 6

Electronic Discovery and Healthcare Litigation

continued from page 5

discussed above are aimed at establishing reasonable criteria based on currently available technologies and providers' common practice experience. According to CMS, the goal will be to establish stricter and more extensive criteria for demonstrating "meaningful use" over time, as anticipated developments in technology and providers' capabilities occur.²³ Under the proposed rule, the Stage 2 criteria will be expanded to include transmission of orders entered using "computerized provider order entry" ("CPOE"), as well as the electronic transmission of diagnostic test results (e.g., blood tests, microbiology, urinalysis, pathology tests, radiology, cardiac imaging, nuclear medicine tests, and pulmonary function tests disease). These expanded criteria will be focused on inpatient as well as outpatient settings.²⁴ At this point, the CMS criteria for Stage 3 (incentive payment year five) are very vague, and understandably so given that the first applicable year will be 2015. For the time being, CMS is indicating that the focus of Stage 3 will be decision support for national high priority conditions, patient access to self management tools, access to comprehensive patient data and improving population health.²⁵

As noted above, ONC issued an Interim Final Rule on December 30, 2009, which also promulgated proposed criteria to achieve "meaningful use" of EHRs for both physician practices and hospitals. For example, a Stage 1 objective for physicians and hospitals will be to implement a system of checks for drug interactions and allergies, as well as whether or not a drug is listed in the hospital or practice formulary. This drug/medication system must include automatic, electronically-generated, real-time alerts (such as a pop-up message at the point of care) for drug allergies and contraindications based on, *inter*

alia, the patient's own medication list, identified allergies, and age.²⁶

The Stage 1 criteria require the drug alerts that are "responded to by a user" be recorded, with the ability to automatically track and generate a report on the number of alerts responded to by that user. Of course, this raises a question as to what will be considered a "response" by a user, and whether the criteria actually require each and every alert be recorded in the computer history, even those where a particular drug was not ordered.²⁷ Even if the computer system does not provide user-friendly access to such an auditable list, the metadata associated with that record may still provide a chronology of what a provider knew and when. Even if a particular drug alert itself is not an issue in the litigation, the information contained in that alert, such as allergy or other medical history, may be relevant information. The metadata created by an EHR system may provide a plaintiff's attorney with clear evidence of what a doctor or nurse should have known about a patient if she had paid careful attention to an alert.²⁸

In addition to the drug interaction and contraindication alerts mentioned above, compliant systems will also have to incorporate five "clinical decision support rules."²⁹ These decision support rules must be designed according to specialty and clinical priorities, and make use of demographic data, specific patient diagnoses, conditions, diagnostic test results and/or patient medication lists, whichever are appropriate in the treatment context. As with the drug alerts, the clinical decision support rules must present themselves in the form of a pop-up message or sound-alert.³⁰ Not only must these alerts be in place, the computer system must be able to automatically track, record,

and generate reports on the number of alerts responded to by a provider. As with the drug alerts, an audit trail of the clinical support messages responded to by a user (whether or not they are acted on) could be key evidence to plaintiffs' attorneys. Plaintiffs' attorneys familiar with system capabilities will be able to cite these regulations in a motion to compel an audit trail, and thereby overcome any objection that the task is too burdensome.

Another proposed requirement in Stage I systems is that a provider must be able to electronically record, modify, and retrieve a patient's list of medical problems over multiple office visits. Furthermore, a provider must be able to electronically reconcile two or more medication lists (compare and merge) into a single medication list that can be displayed in real-time and in electronic format. Providers must also be able to electronically receive a summary of patients from other providers and health organizations including, at a minimum, diagnostic test results, problem lists, medication lists, medication allergy lists, immunizations, and prior procedures.³¹ Some or all of these capabilities are already part of existing EHR systems.

The "meaningful use" criteria must also have capabilities in place to protect electronic health information. The criteria establish that each user must be given a unique name and/or number for "tracking use identity" and establish controls that permit only authorized users to access a patient's electronic health record. Attorneys for providers with similar systems already in place have no doubt been faced with requests for audit trails showing each time a record was accessed, particularly in cases where plaintiff's counsel is attempting to establish a wide range of alleged agents responsible for the plaintiff's care. These audit

trails have been responsible for the new wave of litigation over unauthorized access to electronic health information, which has received wide publicity due to the involvement of celebrity patients. Given the figure cited above that the amount of electronically created data doubles every 18 months, providers will no doubt face an increasing expense in storing all of the information required by the "meaningful use" criteria.

While these proposed criteria for "meaningful use" may sound extensive and revolutionary, especially when compared to a paper chart system, some question whether the scope of the Stage I goals will adequately address the needs and expectations of the providers. One perceived problem is the definition of the term "problem list" for maintaining up-to-date patient information. What individual medical professionals (doctors, nurses, physician's assistants, etc.) consider a "problem list" and how the proposed criteria define a "problem list" are two very different things. Under the regulations, a "problem list" does not include a list of patient complaints, signs and symptoms that are considered the patient's "problems." The "problem list" for "meaningful use" of purposes is not a comprehensive list of all of the patient's signs and symptoms over the course of his or her treatment. Rather, it is simply a list of the patient's "final" diagnoses in ICD-9-CM or SNOMED format.³² In the realities of a clinical setting, it may be some time before the physician "settles" on a diagnosis code for that patient, and under the "meaningful use" criteria, the pre-diagnosis part of the patient's care is *not* considered part of the patient's "problem list."

In providing feedback to CMS, per request, the Certification Commission for Health Information Technology ("CCHIT")³³ has issued a number of comments and criticisms of the proposed criteria, not the least of

which is that the Stage I measures (even if followed to the letter) fall short of defining a "complete" EHR, and fail to match the needs and expectations of doctors and hospitals.³⁴ By way of example, CCHIT questions why the proposed EHR criteria do not address competent electronic management of progress notes. CCHIT suggest that this shortcoming would lead to an EHR that is ultimately unusable and medico-legally unsound. This criticism is understandable in light of the limited scope of a patient's "problem list," referenced above. Without competent management of progress notes and no requirement to record subjective complaints, the EHR criteria fail to address a provider's need to record a patient's own account of his overall health picture.

Despite the potential problems and limitations with the proposed Stage I criteria and EHR systems that may be produced as a result, the amount of electronic health data that will be created, inputted, shared and exchanged for a given patient will continue to grow exponentially. The proposed criteria noted above are just one part of the federal government's push for a major overhaul of medical record keeping over the next five years. And while the information in a patient's medical history should be more reliable and up-to-date as a result, the amount of additional information and metadata (think of the drug alerts-records alone) may be daunting for a litigation attorney faced with a request for the "entire electronic health record."

In the healthcare context and elsewhere, courts and litigators around the country are being challenged by expansive requests for electronically recorded data. As will be discussed below, it will be increasingly important for attorneys to know the changing and developing rules governing electronic discovery, both federally and throughout the states.

Federal Court Impact on Electronic Discovery Practices

*Zubulake v UBS Warburg*³⁵ is generally considered the first definitive case in the country to speak to a wide range of electronic discovery issues. In a series of decisions, *Zubulake I-V*, the United States District Court for the Southern District of New York got the e-discovery ball rolling by specifically addressing the scope of a party's duty to preserve electronic evidence during the course of litigation; data sampling; the ability of a disclosing party to shift the costs of restoring back-up tapes to the requesting party; and sanctions relative to spoliation and/or destruction of electronic evidence.³⁶

Additionally, the court spoke to a lawyer's duty to monitor his or her client's compliance with data preservation and production. Notably, the court found that defense counsel in the case was partially to blame for the underlying document destruction because they had failed in their duty not only to locate relevant information, but also to preserve and timely produce that information. The court stated that attorneys are required to take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched during the litigation process. Ultimately, the court concluded that attorneys are obligated to ensure that all relevant documents are discovered, retained, and produced. According to the court's decision, litigators must also guarantee that identified relevant documents are preserved by placing a "litigation hold" on the documents,³⁷ communicating the need to preserve them, and arranging for the safeguarding of relevant archival media.³⁸

Not surprisingly, the *Zubulake* opinions have been utilized by other courts to assist in their evaluations of e-discovery issues. For instance, in *Wiginton v. CB Richard Ellis, Inc.*, a case involving allegations of nationwide

continued on page 8

Electronic Discovery and Healthcare Litigation

continued from page 7

pattern and practice of sexual harassment, plaintiffs filed a motion for costs of electronic discovery.³⁹ The United States District Court for the Eastern District of Illinois relied on *Zubulake* and enumerated several factors to consider when evaluating whether a party should be compelled to produce information via an electronic discovery request, including: 1) the likelihood of discovering critical information; 2) the availability of such information from other sources; 3) the amount in controversy as compared to total costs of production; 4) the parties' resources as compared to the total cost of production; 5) the relative availability of each party to control costs and its incentive to do so; 6) the importance of the issues at stake in the litigation; 7) the importance of the requested discovery in resolving the issues as stake in the litigation; and 8) the relative benefits to the parties of obtaining the information.⁴⁰

Notably, Judge Scheindin of *Zubulake* wrote another extensive opinion concerning parties' preservation obligations and spoliation issues on January 15, 2010.⁴¹ The opinion indicates that "By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records – paper or electronic – and to search in the right places for those records, will inevitably result in the spoliation of evidence."⁴² Several actions or failures to act were specifically identified as those which would result in a finding of gross negligence in upholding discovery obligations:

After a discovery obligation duty is well established, the failure to adhere to contemporary standards can be considered gross negligence. Thus, after the final relevant *Zubulake* opinion in July 2004, the following failures support a finding of gross negligence,

when the duty to preserve has attached: to issue a written litigation hold; to identify all of the key players and to ensure that their electronic and paper records are preserved; to cease the deletion of email or to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.⁴³

The order also determined that sanctions for evidence spoliation require proof that a party: had control of the evidence at issue as well as an obligation to preserve it at the time it was lost or destroyed; acted with a culpable state of mind; and that the lost or destroyed evidence was not only relevant to the innocent party's claims or defenses, but also that party suffered real prejudice as a result.⁴⁴ Further, the court concluded that "while litigants are not required to execute document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation."⁴⁵

Even more recently, in *Rimkus Consulting Group, Inc. v. Cammarata*,⁴⁶ the District Court for the Southern District of Texas addressed issues of spoliation of evidence and sanctions. The court focused on ascertaining when the deletion of evidence becomes spoliation and determining whether the spoliation merited an adverse inference.⁴⁷ The court noted that spoliation occurs when there is a duty to preserve the information, a culpable breach of that duty occurs, and it resulted in prejudice.⁴⁸ In determining whether spoliation merits an adverse inference instruction, the court indicated that the party seeking the instruction must establish that the party with control over the evidence

had an obligation to preserve it at the time it was destroyed, the evidence was destroyed with a culpable state of mind, and the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support the claim or defense.⁴⁹ The relevance element is further broken down into three parts: 1) whether the evidence is relevant to the lawsuit generally, 2) whether it would have supported the inference sought and 3) whether the non-destroying party suffered prejudice from the destruction.⁵⁰

E-Discovery and the Federal Rules of Civil Procedure

Given the overwhelming trend toward electronic data storage (which, in a healthcare context, will only grow given the goals of the stimulus package) it was inevitable that formal changes would occur in the rules governing discovery of electronic data. The Federal Rules of Civil Procedure were amended in December 2006 to specifically address e-discovery and have become the model for changes in discovery rules at the state level.

Both Rule 16, Pretrial Conferences; Scheduling Management and Rule 26, General Provisions Governing Discovery; Duty of Disclosure, require that issues pertaining to the disclosure and discovery of electronic information be addressed by the parties. Rule 33, Interrogatories to Parties, specifically provides that interrogatories involving a review of records should include a search of any electronically stored information. Rules 34 and 35 pertaining to production of documents provide that documents need only be produced in one form, either hard-copy or electronic. Accordingly, attorneys and their healthcare clients should work closely as new electronic record systems are

put in place to streamline the seemingly inevitable request for records with a plaintiff's counsel's letterhead.

Furthermore, Rule 37 addresses sanctions for failure to make disclosure or cooperate in discovery. The Rule does provide some protection for failing to produce information due to loss occurring because of routine operation of an entity's computer system if the entity took reasonable steps to preserve the information at issue. Prior to these amendments, the Rules did not specifically reference electronic data in any way.

Status of State E-Discovery Rules

A majority of states have modified their respective rules of civil procedure, most in a manner which largely tracks the federal rules.⁵¹ Many other states have indicated an intention to update their rules to address e-discovery issues.⁵² There are also a number of states, such as Alabama, Pennsylvania, and Rhode Island, that have not addressed e-discovery issues to date.

Texas was the first state to amend its discovery rules to address electronically stored information. It added two sections to its Rules way back in 1999. Rule 193.4(d), Privilege not Waived by Production, allows a party to assert a claim of privilege within ten days of inadvertent production, to material or information produced inadvertently without intending to waive the privilege.⁵³ Rule 196.4, Electronic or Magnetic Data, provides that a party requesting production of electronic data must specifically request the data, specify the form in which it wants the data produced, and specify any extraordinary steps for retrieval and translation. Unless ordered otherwise, the responding party need only produce the data reasonably available in the ordinary course of business in reasonably useable form.⁵⁴

California is another state that has already amended its rules. On June 29, 2009, Arnold Schwarzenegger, Governor of California, signed into law AB 5 as California's first set of statutes specifically designed to address electronic discovery. The law added two new statutes to California's Code of Civil Procedure ("CCP"), and amended nineteen pre-existing CCP sections. The changes largely track the federal rules. The new statutes subject ESI to discovery automatically, impact privilege considerations, change discovery procedures relative to requests directed to both parties and non-parties, address cost shifting, and specify that sanctions can be imposed for non-compliance in discovery of electronically stored information.⁵⁵

Pennsylvania is one of the states which has not adopted the federal rules or specifically amended its discovery rules. However, a recent opinion suggests that the federal approach will be followed in Pennsylvania state courts. In *Brooks v. Frattaroli*,⁵⁶ the Lebanon County Court of Common Pleas granted the defendant's motion for a protective order, finding the plaintiff's discovery request to enter the defendant's property to inspect and copy computer files was overly broad. Noting a relative dearth of precedent governing discovery of ESI in Pennsylvania, the court drew on the decisions of federal courts and the recent changes to Federal Rule of Civil Procedure 34 to arrive at a balancing test that weighed the defendant's right to privacy against the plaintiff's desire to determine the truth. The court utilized five factors in its analysis, including: the scope of the request, confidentiality/privacy, the history of discovery in the litigation, costs, and the type of case involved.

In reaching its conclusion, the *Brooks* court noted the analysis in *Young v. Pleasant Valley School District*,⁵⁷ where a plaintiff sought to examine a school district's computers. In that case, the court denied the request, finding that it would cause a range of

privacy concerns for the district, its students and their parents and that the supervision required to ensure the parties' privacy would be unbearably expensive and burdensome. The Pennsylvania state court also looked to *Bianco v. GMAC Mortgage Corp.*,⁵⁸ a case brought in the United States District Court for the Eastern District of Pennsylvania, where a plaintiff requested access to the defendant's employee's laptop for inspection. The *Bianco* court sided with the defendant, finding that it was improper to order an intrusive examination on mere suspicion of discovery misconduct.

Generally, state courts seem to be modeling their e-discovery rules after the Federal rules. In states where the rules have not been changed, or changed in only limited respects, state courts are relying heavily on the federal rules and federal court precedent addressing e-discovery issues. Yet, it is important for attorneys to understand that there are often important distinctions between the federal rules and those of the states. For example, unlike the federal rules, the Arizona Rules of Civil Procedure lack any provision directing the parties to address electronic discovery early in a case, if necessary, to get such issues resolved promptly by a court. Likewise, unlike the federal rules, the Arizona rules do not require that the parties confer about electronic discovery matters, including the form of production and relative accessibility of the information, before disclosing such information.⁵⁹

Federal Case Law Addressing Discovery Issues

This is still a burgeoning area of the law, and as a result there are not a large number of published cases interpreting the new Federal Rules of Civil Procedure, e-discovery generally and, more specifically, e-discovery in the context of EHR or other ESI in the healthcare setting. However, it is expected that published opinions concerning discovery requests for EHRs

continued on page 10

Electronic Discovery and Healthcare Litigation

continued from page 9

will increase with proportion of providers using electronic record systems.

It is worth noting that that one federal court has issued a decision regarding inadvertent production of privileged ESI. This case actually post-dates the amendments to the Federal Rules of Civil Procedure. Notably, the result is likely different than had the case been decided under the Texas Rules of Civil Procedure, which provides a specific rule regarding inadvertent disclosure of privileged information. In *Amersham Biosciences Corp. v. Perkinelmer, Inc.*,⁶⁰ the District Court of New Jersey discussed what "reasonable precautions" must be taken when dealing with privileged ESI. The court was asked to decide whether reasonable precautions were taken in relation to the inadvertent disclosure of over 500 privileged e-mail documents that were deleted within subfolders when converted to CD, but remained embedded in the larger folder when converted to single image files.

The court held that if the confidential or privileged nature of the documents was apparent on the face of the documents after their conversion from their native form to single image files, then the final spot check conducted by the disclosing party may have been reasonable, and that the disclosure may not have waived the privilege at issue. However, there was a factual discrepancy concerning whether the receiving party went beyond "the confines of the fact of the documents and uncovered hidden information,"⁶¹ i.e. metadata. The court determined that further factual inquiry regarding the specifics of whether the data was facially apparent or required further investigation of hidden information was required, and therefore, remanded the matter.⁶²

Consequently, it would appear that reasonable precautions may require

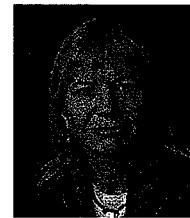
counsel to review each electronically stored document at every stage of conversion to a discoverable format, whether on disk or a paper print out of the selected data, in order to ensure that non-discoverable metadata is actually cleared before production occurs. In other words, reasonable precautions could be somewhat elevated when dealing with ESI. But, if the disclosing party knows that metadata exists and takes reasonable precautions to erase this confidential information at every stage of the pre-disclosure process, it appears that a court will be more likely to find that a privilege was not waived, and the disclosure is more likely to be deemed inadvertent.

Conclusion

The rules and case law governing electronic discovery throughout the United States, in all areas of the law, are still in the developmental stages. While healthcare's relatively slow transition to EHR may have afforded litigators the ability to adopt a "take it as it comes" approach, the future will not present that luxury. Given the Medicare incentives and adjustments alone, EHR systems will be adopted by providers at a faster rate than they ever have been before. Producing an EHR in medical malpractice litigation, or otherwise, will no longer be the exception, but the norm. Although the above-referenced cases and e-discovery rules are not focused only on medical records, understanding the judicial analysis of similar electronic data issues will help attorneys anticipate the key arguments, and better serve their clients over the next five years and beyond.

Further, though not addressed specifically in this article, given the rules and related case law, attorneys should ensure that their healthcare clients have appropriate records retention and destruction policies in

place because destroying certain information can increase legal exposure. Conversely, keeping carelessly written or long outdated information can increase legal exposure. An important element in this process is the implementation of a policy regarding how to stop destruction of data once litigation is reasonably anticipated and when a litigation hold has been requested.



Anna M. Bryan

is a partner in the Litigation Department at White and Williams LLP in Philadelphia, PA. She works with

hospitals, nurses and physicians in various areas of medical negligence across the State and has developed a special expertise in hand surgery and orthopedic surgery cases. Ms. Bryan has served as lead counsel in numerous cases taken to verdict in medical negligence cases.

After receiving her professional nursing license in 1975, she received both her B.S. in 1978 and her M.S. in 1979 from the University of Pennsylvania.

Thereafter, she completed all course work and a significant portion of her Doctoral Dissertation, in Health Education, with a component of Public Health course work, at Temple University where she received her J.D. in 1988.

Ms. Bryan teaches Residents at Temple University Medical School and has been invited to give numerous presentations to various healthcare groups, individuals and academic institutions over the years. She continues to hold her professional nursing license.

Ms. Bryan is a member of the Pennsylvania Bar Association and New Jersey Bar Association. She is also a Fellow of the Litigation Counsel of America, a trial lawyer honorary society comprised of less than one-third of one percent of American lawyers. Fellowship

to the LCA is highly selective and by invitation only. Ms. Bryan was selected in a survey of her peers as a Pennsylvania "Super Lawyer" by *Law & Politics* magazine in 2005 and 2009. She may be reached at bryana@whiteandwilliams.com.



Debra A. Weinrich is an associate in the Litigation Department at White and Williams LLP in Philadelphia, PA and is a member of the

Healthcare practice group. She focuses her practice on medical malpractice defense and primarily works with physicians, nurses, other healthcare personnel as well as hospitals and physicians' practice groups.

Ms. Weinrich received her B.S.N. from Thomas Jefferson University in 1993, where she was inducted into the International Honor Society of Nursing, Sigma Theta Tau. She practiced as a Registered Nurse for approximately 10 years, principally in the area of Maternal-Newborn Services, and was certified in Inpatient Obstetrics. She maintains a nursing license in both Pennsylvania and New Jersey.

In 2004, Ms. Weinrich received her Juris Doctorate from Rutgers University School of Law – Camden, where she received a legal writing award, as well as a Pro Bono Service Award. Ms. Weinrich also served as Articles Editor for the Rutgers-Camden Journal of Law and Religion.

She is a member of the Lawyers' Club of Philadelphia and the Philadelphia Area Society for Healthcare Risk Management. She may be reached at weinrichd@whiteandwilliams.com.



Edward F. Beitz is an associate in the Litigation Department at White and Williams LLP in Philadelphia, PA and is a member of the

Healthcare Group. His practice focuses on medical malpractice defense. Mr. Beitz received his B.A., magna cum laude,

from LaSalle University in 2002, and his J.D. from Rutgers University School of Law-Camden in 2006. As a law student, he served as the Lead Articles Editor on the Rutgers Journal of Law and Religion. Mr. Beitz also participated in Rutgers' Hunter Moot Court Tournament, where he placed as a finalist and was appointed to the National Moot Court Team. He may be reached at beitze@whiteandwilliams.com.

Endnotes

- ¹ <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm>.
- ² A gigabyte (GB) equals 1,000,000,000 bytes. One hour of High-Definition video, recorded on a digital video camera at its highest quality setting, is approximately 7 gigabytes. Bohn, RE and Short JE, *How Much Information? 2009 Report on American Consumers*, at <http://hmi.ucsd.edu/howmuchinfo.php>.
- ³ IDC: Digital Data to Double Every 18 Months, *Information Management Journal*, (Sep/Oct 2009), available at: http://findarticles.com/p/articles/mi_qa3937/is_200909/ai_n39233493/?tag=content;col1.
- ⁴ NCHS Health E-Stat, available at the Centers for Disease Control and Prevention website at http://www.cdc.gov/nchs/data/hestat/emr_ehr/emr_ehr.htm.
- ⁵ The survey defined a fully functional EHR system as including capabilities for medical history and follow-up, orders for tests, prescription and test orders sent electronically, patient demographic information, patient problem lists, clinical notes, orders for prescription and viewing laboratory, imaging results warnings of drug interactions or contraindications, highlighting of out-of-range test levels, electronic images returned, and reminders for guideline-based interventions.
- ⁶ The Federal Rules of Civil Procedure, as amended in December 2006, include references to "electronically stored information" but do not include a definition.
- ⁷ Shorter Oxford English Dictionary on Historical Principles, (6th ed., 2007). *The Sedona Conference Glossary: E-Discovery & Digital Information Management 2nd Ed.* (Dec. 2007), http://www.thesedonaconference.org/dlt/Form?did-TSCGlossary_12_07.pdf, defined metadata as "data typically stored electronically that describes characteristics of ESI." The glossary adds that metadata "can describe how, when, and by whom ESI was collected, created, accessed, modified and how it is formatted."
- ⁸ *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 547 (D. Md. 2007).
- ⁹ See Department of Health and Human Services, Interim Final Rule, 42 CFR Part 170 (January 13, 2010), which can be downloaded at <http://edocket.access.gpo.gov/2010/pdf/E9-31216.pdf>.

- ¹⁰ Electronic Health Records are also often referred to as electronic medical records ("EMR"). The terms have generally been considered synonymous by practitioners. However, it is worth noting that the National Alliance for Health Information Technology ("NAHIT") has established definitions for electronic medical records ("EMR") and electronic health records ("EHR"). NAHIT has an "electronic medical record" as the "electronic record of health-related information on an individual that is created, gathered, managed, and consulted by licensed clinicians and staff from a single organization who are involved in the individual's health and care." NAHIT has defined an "electronic health record" as "the aggregate electronic record of health-related information on an individual that is created and gathered cumulatively across more than one health care organization and is managed and consulted by licensed clinicians and staff involved in the individual's health and care." See Neal, Houston, *EHR vs. EMR – What's the Difference?* available at <http://www.softwareadvice.com/articles/medical/ehr-vs-emr-whats-the-difference/>.
- ¹¹ The HITECH Act, part of the American Reinvestment and Recovery Act of 2009, amended the Public Health Service Act to include numerous definitions and provisions concerning Health Information Technology and Quality. See 42 U.S.C.A. § 300jj, *et seq.*
- ¹² 42 U.S.C.A. § 300jj(13).
- ¹³ It should be noted that, for both attorneys and their healthcare clients, it is not always clear what should be or needs to be produced in response to a discovery for electronic health records. For example, while reports interpreting radiology, pathology, lab values or fetal monitoring strips are considered part of the patient's health record, the actual images, pathology slides, specimens and/or monitoring strips themselves are generally not. While those items certainly relate to and document information regarding the care and treatment provided, a separate subpoena and/or discovery request is generally required to obtain those pieces of information. The same holds true for related billing records. These issues may present themselves when healthcare clients are deciding how to produce health records in an electronic format, and what should be included.
- ¹⁴ See DHHS Interim Final Rule, *supra* endnote 9, at page 2040.
- ¹⁵ Centers for Medicare and Medicaid Services Fact Sheet, June 16, 2009, available at: <http://www.cms.hhs.gov/apps/media/press/factsheet.asp?Counter=3466>.
- ¹⁶ *Id.* The incentives are scaled downward each year, with maximum payments of \$12,000; \$8,000; \$4,000; and \$2,000 in the second, third, fourth, and fifth years respectively. For early adopters whose first payment year is 2011 or 2012, the maximum payment is \$18,000 in the first year.
- ¹⁷ *Id.*
- ¹⁸ *Id.*
- ¹⁹ *Id.*

continued on page 12

Electronic Discovery and Healthcare Litigation

continued from page 11

- ²⁰ U.S. Department of Health and Human Services' News Release, *CMS and ONC Issue Regulations Proposing a Definition of 'Meaningful Use' and Setting Standards for Electronic Health Record Incentive Program*, available at: <http://www.hhs.gov/news/press/2009pres/12/20091230a.html> (December 30, 2009).
- ²¹ See generally DHHS Interim Final Rule, *supra* endnote 9.
- ²² *Id.*
- ²³ See U.S. Department of Health and Human Services' News Release, *supra* at endnote 17.
- ²⁴ See generally DHHS Interim Final Rule, *supra* endnote 9.
- ²⁵ *Id.*
- ²⁶ See DHHS Interim Final Rule, *supra* endnote 9, at page 2026.
- ²⁷ *Id.*
- ²⁸ Medical professionals should be aware of the impact metadata will have on professional liability cases. At least some physicians seem to be taking note of this. One study published in the *Journal of the American College of Surgeons* concluded that the metadata associated with EHRs will be increasingly used to discredit physicians during medical malpractice litigation. See *Electronic Medical Record Metadata: Uses and Liability*, *Journal of the American College of Surgeons*, Volume 206, Issue 3, 405-11.
- ²⁹ See DHHS Interim Final Rule, *supra* endnote 9, at page 2027.
- ³⁰ *Id.*
- ³¹ *Id.* at page 2028.
- ³² This will be upgraded to ICD-10-CM for purposes of the Stage 2 criteria, which will bring it in line HIPAA's Code Sets Standards. ICD-10-CM is also being mandated for reimbursement.
- ³³ CCHIT is a nonprofit, 501(c)3 organization, whose mission statement includes promoting and accelerating the adoption of health information technology.
- ³⁴ Comments on the Interim Final Rule on Standards, Implementation Specifications, and Certification Criteria for EHRs, available at <http://www.cchit.org/about/comments-testimony/ifr-comments>.
- ³⁵ See *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003), *Zubulake v. UBS Warburg*, 216 F.R.D. 280 (S.D.N.Y. 2003), *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003), *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004).
- ³⁶ The *Zubulake* case involved allegations of employment discrimination (sex discrimination and retaliation), and was overseen by Judge Shira A. Scheindin, now famous for her decisions in the case. Judge Scheindin issued a series of e-discovery decisions and ultimately concluded that Defendant UBS willfully deleted relevant emails. The court gave the jury an adverse inference instruction, indicating that if the jury found that the defendant deleted the emails at issue, it could assume that the emails, destroyed after the Plaintiff's complaint was filed, would have negatively impacted the defendant's case. The jury found UBS discriminated against the Plaintiff and awarded more than \$29 million in damages (\$20.1 million in punitive damages and \$9.1 million in compensatory damages). Ultimately, the parties settled the matter for an undisclosed sum.
- ³⁷ A litigation hold is a suspension of an organization's document retention and destruction for documents that may be relevant to a lawsuit that has been filed or for litigation that may be reasonably anticipated. Its purpose is to ensure that relevant information is not destroyed and that personnel are advised of the need to preserve data given the potential and/or pending litigation.
- ³⁸ See *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004).
- ³⁹ 229 F.R.D. 568 (N.D. Ill. 2004).
- ⁴⁰ *Id.*
- ⁴¹ See *Pension Comm. of Univ. of Montreal Pension Plan v. Bank of Am. Secs., LLC*, 2010 WL 184312 (S.D.N.Y. Jan 15, 2010) (Amended Order).
- ⁴² *Id.*
- ⁴³ *Id.*
- ⁴⁴ *Id.*
- ⁴⁵ *Id.*
- ⁴⁶ 2010 WL 645253 (S.D. Tex. Feb. 19, 2010).
- ⁴⁷ An adverse inference instruction informs a jury that if it finds that a party fails to produce evidence that was under that party's control and reasonably available to that party and not reasonably available to the adverse party, then the jury may infer that the evidence was unfavorable to the party who could have produced it and did not. It is given in cases of suspected suppression, hiding or destruction of evidence.
- ⁴⁸ *Id.* at 5.
- ⁴⁹ *Id.* at 7.
- ⁵⁰ *Id.*
- ⁵¹ For instance, Arizona, California, Indiana, Iowa, Maryland, Minnesota, New Jersey, and Utah have all amended their respective Rules to largely mirror the Federal amendments.
- ⁵² States such as New York, North Carolina, South Carolina and Vermont have all considered, or are still in the process of considering, changes to their respective rules of civil procedure.
- ⁵³ See Tex. R. Civ. P. 193.3(d).
- ⁵⁴ See Tex. R. Civ. P. 196.4; 61 Texas Bar Journal 1140, 1158-1159 (December 1999).
- ⁵⁵ See e.g., CCP §§ 1985.8(b), 1985.8(c)(1), 1985.8(e), 1985.8(f), 1985.8(g), 2016.020(d)-(e), 2031.030(a)(2), 2031.050(a), 2031.060(c)-(f)(1)-(4), 2031.101(a)(2), 2031.280(c)-(d)(1)-(2), 2031.280(d)(1), 2031.280(e), 2031.310(d)-(f), and 2031.310(f).
- ⁵⁶ PICS Case No. 09-1709 (C.P. Lebanon Oct. 5, 2009).
- ⁵⁷ 2008 W.L. 2857912 (M.D. Pa. 2008).
- ⁵⁸ 2008 W.L. 4661241 (E.D. Pa. 2008).
- ⁵⁹ See generally, Az. R. Civ. P.
- ⁶⁰ 2007 WL 329290 (D. N.J. 2007).
- ⁶¹ *Id.* at 5.
- ⁶² *Id.* at 5-6.

The Health Law Section has many opportunities for your involvement. Currently the **HLS liaison to the AIDS Coordinating Committee** is available and may be of interest to you. A liaison participates in meetings and communicates relevant information back to the Section's Council. It's a great way to serve the Section and meet others who are active in the ABA. For more information about it, please visit <http://www.abanet.org/AIDS/home.html>.

If you have questions about this opportunity, please contact Simeon Carson, Associate Director, at carsons@staff.abanet.org or at (312) 988-5824. If you would like to apply for this position, please submit your resume to Simeon at carsons@staff.abanet.org.