



The health law solution.

June 27, 2008

Virginia's Proposed Electronic-Discovery Rules: *Healthcare Providers Should Prepare for the Inevitable*

CLIENT ADVISORY

The rapid advance of technology continues to have a dramatic impact on the delivery of healthcare, and on the malpractice litigation that occasionally follows. Although Virginia lacks formal rules of evidence, there is an established body of case law that addresses the most common discovery issues that arise in civil litigation. In addition, those involved in preparing for and handling medical malpractice suits in Virginia have long been able to rely on the relative certainty of Virginia's Medical Malpractice Act¹, the quality assurance privilege², and Rules of the Supreme Court of Virginia³, to provide some guidance and predictability.

As we enter the digital age, some legal uncertainty has resulted. The federal courts and numerous individual states are drafting rules specifically to address electronic discovery issues in civil litigation. These changes are coming to Virginia in the near future and the time to prepare is now.

Because state law governs most medical malpractice claims in Virginia, even the recent changes to the Federal Rules of Civil Procedure regarding electronic discovery have had little practical significance in day-to-day handling of anticipated or pending medical negligence litigation to date. But this paradigm is changing as the states follow the lead of the Federal Rules and adopt specific provisions for electronically stored information ("ESI").

Plaintiff's and defense attorneys are also increasingly focusing on the availability of electronic data as another source of evidence in litigation. Risk managers, claims managers, and insurance industry personnel are well-advised to anticipate this issue as well.⁴ Electronic discovery is alive and well at the federal level and is now poised to become a significant issue in Virginia courts.

On October 1, 2007, the Advisory Committee on the Rules of Court of the

¹ Virginia's Medical Malpractice Act is codified at Va. Code § 8.01-581.1 et seq. The provisions of the Act have generally been interpreted consistently by the Virginia Courts, with some rulings presenting unexpected results.

² Virginia Code Section 8.01-581.16 & 17 codify the quality assurance privilege.

³ See Va. Sup. Ct. Rule 1:1 et seq.

⁴ The issue has garnered some attention in Virginia. For example, the 2008 Spring Program of the Virginia Chapter of American Society for Healthcare Risk Management recently addressed issues involved with electronically stored information ("ESI"), in part highlighting considerations in electronic discovery for risk managers throughout the Commonwealth.



Hancock, Daniel, Johnson & Nagle, PC (HDJN) provides assistance and guidance to health care providers in virtually all legal matters affecting healthcare. Generally, these include corporate, employment, administrative, and transactional matters; litigation; and governmental affairs.

Judicial Council of Virginia published Tentative Draft of Electronic Discovery Rules for Virginia (“Draft ESI Rules”).⁵ The Draft ESI Rules implement themes specifically addressed in the recent amendments to the Federal Rules of Civil Procedure directed at electronic discovery.⁶

The Draft ESI Rules are not yet implemented and after final review by the Advisory Committee, the Supreme Court of Virginia will determine the extent that electronic discovery rules should be implemented in the Commonwealth.⁷ Whatever the final form of Virginia’s electronic discovery rules, the implementation of rules involving electronic discovery will shift the litigation paradigm towards the electronic issues already being addressed by federal courts.⁸ With the increased importance of electronic medical records⁹ and the proliferation of electronically stored information in all aspects of healthcare, electronic discovery will be an issue of critical importance for healthcare providers.

This article looks to the provisions in the Draft ESI Rules and compares the

draft rules to parallel issues in the federal rules, highlighting the application of these rules and lessons from instructive case law. The article will also address some practical concerns of significance for those involved in defending medical malpractice cases in Virginia.

What is Discoverable?

The purpose of pretrial discovery in civil litigation is “to disclose all relevant and material evidence before trial in order that the trial may be an effective method for arriving at the truth.”¹⁰ The search for truth in a medical negligence case is focused on medical documentation and early discovery typically begins with an authorization and release from a plaintiff requesting “all records,” or similarly, an attorney issued subpoena *duces tecum* for the same.¹¹ The patient will typically cite statutes that broadly authorize him or her to access his or her personal health information.¹² Increasingly, the laundry list of “documents and things” requested by such an authorization or subpoena is expansive and includes electronic data.¹³

⁵ See Letter to the Bench and Bar of Virginia, from The Advisory Committee on Rules of Court, dated October 1, 2007 (hereinafter “Draft ESI Rules”) (available at <http://www.courts.state.va.us/scv/reports/ediscovery.pdf>).

⁶ See *id.* Although the Draft ESI Rules only mention the recent amendments to the Federal Rules of Civil Procedure in passing, the principles they reflect would seem to directly relate to provisions implemented at the federal level.

⁷ The Judicial Council of Virginia approved the Draft ESI Rules with a minor amendment in June 2008. The final step in the process is approval by the Supreme Court of Virginia.

⁸ Even in the unlikely event the Supreme Court of Virginia declines to adopt any version of the Draft ESI Rules, healthcare providers will be confronted with an increasing number of requests for ESI. The federal rules will then be the most persuasive Framework for analyzing electronic discovery issues.

⁹ Virginia was recently included as one of the communities selected to work with the Centers for Medicare & Medicaid services to advance the use of Electronic Health Records in a national demonstration. See News Release, HHS Secretary Announces 12 Communities Selected to Advance Use of Electronic Health Records in First Ever National Demonstration, June 11, 2008.

¹⁰ *Little v. Cooke*, 274 Va. 697, 717 (2007) (citing *Guilford Nat’l Bank of Greensboro v. Southern R. Co.*, 297 F.2d 921, 924 (4th Cir. 1962); *Hickman v. Taylor*, 329 U.S. 495, 516, 67 S. Ct. 385, 91 L. Ed. 451 (1947)).

¹¹ See Va. Sup. Ct. Rule 4:9.

¹² See Va. Code § 32.1-127.1:03; 45 C.F.R. 164.524.

¹³ For example, “Any and all medical records, documents and things kept in any form whatsoever, including but not limited to, any documents, office records, prescription records, correspondence, hospital records, progress notes, orders, consultations, nursing notes and flowsheets, therapy records, laboratory and pathology reports, x-ray films, MRIs and CTs, all radiological reports, mental health treatment records, medication records, photographs, EKG and EEG studies, disability applications and evaluations, and billing records.” The scope of this request includes virtually every type of format, including electronic information, which may have been produced regarding a patient.



HDJN is one of the largest Virginia law firms primarily focusing its practice on the needs of the healthcare industry.

Healthcare providers have traditionally responded to these authorizations and subpoenas, by providing only those documents that they have deemed to comprise the “official medical record.” Sometimes, more expansive requests are responded to with an objection or a motion to quash a subpoena. Other times, the excess verbiage is simply ignored and the response is limited to the data stored in the medical records or health information department to whom the subpoena is directed. This issue is one where healthcare providers are wise to seek legal counsel, evaluate their internal procedures, and proceed cautiously.

In this age of pervasive digital technology in healthcare, there often exists other patient specific data that does not find its way to the “medical record.” For example, electronic data about lab results, computerized monitoring systems, medication access machines, emails, etc., often exists in some format in the healthcare provider’s digital world, but is not produced even when specifically requested - because it is not considered part of the “medical record.”

This analysis is challenging as the law is not crystal clear as to whether the patient has a specific right to access this information in response to an authorization and release, or an attorney issued subpoena. The analysis changes further when a case is in active litigation and a specific Request for Production¹⁴ is propounded to the defendant healthcare provider requesting such information. It is at this stage that it

is expected that the proposed electronic discovery rules, as interpreted and applied by circuit court judges across the Commonwealth, will come into play.¹⁵ Until that time, healthcare providers are advised to carefully evaluate their responses to patient authorization requests for electronic information outside the designated medical record.

Electronic Discovery in Medical Malpractice Litigation

To date, medical malpractice litigation has largely escaped consideration as a frontier for electronic discovery. There is a perception that electronic discovery is relevant only in federal litigation; the perception is perpetuated because medical malpractice litigation occurs primarily in state courts which do not have specialized electronic discovery rules and because only recently has electronic information begun to proliferate widely in the provision of patient care. At best, many healthcare providers have approached electronic discovery issues in medical malpractice on a piecemeal basis, responding only as immediately necessary.

When discovery requests for electronic information are propounded in a pending case, the healthcare provider can be caught off guard when the defense team begins to ask the hard questions in an effort to ensure compliance with the request. What do we do with this particular request for specific electronic information? Or, how do we obtain this particular piece of information?

¹⁴ See Va. Sup. Ct. Rule 4:9. The scope of material obtainable through a Request for Production is expansive and is governed by the language of Va. Sup. Ct. Rule 4:1, “Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter.”

¹⁵ The Draft ESI Rules will also break out the provision for an attorney issued subpoena *duces tecum* from the provision enabling a Request for Production, establishing Rule 4:9A for subpoenas *duces tecum*.



Lawyers at HDJN have diverse backgrounds and varying specialties and represent decades of experience in providing legal advice to health care providers.

The Draft ESI Rules represent an excellent opportunity for risk managers and other healthcare providers to get ahead of the curve in electronic discovery before it becomes a significant issue in state court litigation. Additionally, preparing for the proposed state electronic discovery rules will allow healthcare providers to be prepared for the issues which crop up during infrequent, but inevitable, federal litigation.

The authors propose that there are five key areas of consideration for healthcare providers when looking at the Draft ESI Rules for Virginia and planning for their implementation: 1) understanding the definition of electronic information and knowing what must be produced; 2) identifying information that is not reasonably accessible; 3) preparing for good cause challenges; 4) leveraging cost shifting provisions; and 5) understanding the limited protections for routine destruction of electronic information.

1) Defining “Electronic Information”

The Draft ESI Rules specifically include electronically stored information within the scope of discovery. The new rules now specifically state that parties may obtain discovery by the “production of documents, electronically stored information, or things.”¹⁶ The addition of this language is not a particularly novel development. The discoverability of ESI in Virginia has been occurring between parties for years even without this rule. However the language of the proposed rule adds some clarity and force to the arguments seeking production of electronic data.

“Electronically stored information” is broad and can encompass a wide variety of data that exists in the healthcare setting. In Virginia, email, electronic documents, and other electronically stored information have long been recognized by parties as an important component of proof in civil litigation.

For example, in a bench trial before the Loudoun County Circuit Court in 2005, the court entered an award for \$1,654,833.00, based in part upon email correspondence between the defendants.¹⁷ The probative value of electronic information (particularly email) cannot be overlooked and, hence, must be a consideration for risk managers and healthcare providers. As society becomes more and more familiar with the concept of the durable electronic fingerprint, electronic information will become more and more useful for litigants as a source of discoverable information and ultimately a source of proof.¹⁸

Beyond labeling ESI generally as discoverable, the Draft ESI Rules go on to further identify the scope of discovery allowed with electronic information and how the courts will address issues of complex electronic discovery. First of all, “A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.”¹⁹ Second, when a party claims that information is not reasonably accessible, “On a motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably

¹⁶ See Draft ESI Rules 4:1(a) (modifying Va. Sup. Ct. Rule 4:1(a) to add “electronically stored information”).

¹⁷ See *James, Ltd. v. Saks Fifth Avenue, Inc.*, 67 Va. Cir. 126 (Loudoun County 2005) (reversed in part on other grounds by *Saks Fifth Avenue, Inc. v. James, Ltd.*, 272 Va. 177 (2007) (acknowledging that email comprised a component of proof in the case)).

¹⁸ For example, metadata is increasingly becoming a significant consideration in electronic discovery, even though it only contains “data about data.” See W. Lawrence Wescott II, *The Increasing Importance of Metadata in Electronic Discovery*, 14 RICH. J.L. & TECH. 10 (2007) (available at <http://law.richmond.edu/jolt/v14i3/article10.pdf>).

¹⁹ See Draft ESI Rule 4:1(b)(7)(emphasis added); see also Section 2(A) *infra*.



HDJN clients benefit from our distinctive set of skills, resulting in prompt, effective legal service.

accessible because of undue burden or cost.”²⁰ Third, even if a party is able to demonstrate that information is not reasonably accessible, “the court may nonetheless order discovery from such sources if the requesting party shows good cause.”²¹ Fourth, “The court may specify conditions for discovery, including the allocation of reasonable costs thereof.”²² These principles are important because they define the scope of issues with which Virginia courts (and ultimately healthcare defendants) will be confronted.

When anticipating electronic discovery requests, and when developing electronic data systems, healthcare providers and their counsel should become familiar with the many types of electronic data that may be stored about a given patient.

2) Discovering the “Reasonably Accessible”

“Reasonable accessibility” is the threshold for determining whether electronically stored information is subject to discovery at all. The language of the rule is simple, “A party need not provide discovery of electronically stored information from sources that the party identifies as **not reasonably accessible** because of undue burden or cost.”²³ While this may sound like a powerful tool for parties to use to shield themselves from electronic discovery requests, in order to take advantage of the provision regarding the disclosure of electronic information, a party must be able to: 1) identify the information and 2) demonstrate why it is not reasonably accessible based on undue burden or cost. In many instances, demonstrating that information is not reasonably accessible will prove difficult in the context of healthcare

information; however, this standard may prove to be effective at minimizing the burden of discovery, particularly regarding electronic information outside of the four corners of the medical record.

A) Identifying What You Cannot Produce

Under the proposed rules, before a party can make a claim that information is not reasonably accessible, the electronic information must first be identified. Although this requirement appears innocuous, as will be noted later, the failure to identify electronic information (and the failure to preserve that information) can have serious consequences.²⁴ The requirement of identification of the electronically stored information is analogous to the requirement that a party disclose a description of the substance of a document when claiming privilege under Rule 4:1(6).

When a party withholds information that is otherwise discoverable under the Virginia Rules on the basis of privilege, the party is required to expressly claim the privilege, describe the nature of the documents, communications, or things not produced or disclosed in a manner that enables other parties to assess the applicability of the privilege (and allow the court to rule intelligently on the matter).²⁵ Identification serves another purpose, in that it allows the opposing party to gather basic information that will be used to challenge the claim that the information is not reasonably accessible. This quid pro quo of exchange of information ensures that both parties are able to fairly present their perspectives on the discovery of claimed inaccessible electronic information.

²⁰ See Draft ESI Rule 4:1(b)(7)(emphasis added); see also Section 2(B) *infra*.

²¹ See Draft ESI Rule 4:1(b)(7); see also Section 3 *infra*.

²² See Draft ESI Rule 4:1(b)(7); see also Section 4 *infra*.

²³ See Draft ESI Rule 4:1(b)(7)(emphasis added).

²⁴ See Section 5, *infra*.

²⁵ See Va. Sup. Ct. Rule 4:1(6).



In-depth, up-to-date knowledge of the law along with responsiveness and personal attention to our clients are priorities at HDJN.

In order to identify ESI, healthcare providers and risk managers must be able to understand the full spectrum of electronic information that is potentially available. Outside of the healthcare context, electronically stored information is frequently confined to computers and computer systems involved in the core business of the party. But healthcare providers are confronted with numerous sources of potential ESI.

For example, telemetry devices may directly output their results to a screen which is used by the nursing staff to log vital signs, but the same equipment may keep a real time digital log of vital signs which is more extensive than the printout in the medical record. Handheld devices used by physicians may contain electronic notes, no different than a handwritten notebook, but contained in electronic form and not included in the medical record. Risk managers confronted with litigation need to quickly be able to triage the process used to provide care in each individual case to identify potential sources of ESI.

A significant portion of “process mapping” can and should occur in advance, but the individualized habits of a healthcare provider or the particular care provided to an individual patient mean that the ESI issues involved may be unique to the particular situation at hand. The healthcare provider must be prepared

to gather all the relevant information, produce what can be produced, and identify what information is not reasonably accessible.

B) Why It Cannot Be Produced

The standard of reasonable accessibility has been generally governed by the type of format that contains the electronically stored information. The seminal case for defining what electronically stored information is reasonably accessible is based on a series of decisions on ESI from the Southern District of New York, *Zubulake v. UBS Warburg*.²⁶ In *Zubulake*, the Court reasoned that electronic storage systems that were more complex and made information more difficult to obtain tipped in favor of inaccessibility; ultimately, determining that particular categories of storage mediums were not reasonably accessible.²⁷

Using storage format as a basis for determining what information is reasonably accessible may be effective with information that is backed up, such as email and other electronic databases, but may not be as effective with healthcare ESI and electronic data that is not stored in a backup format.

Accessibility of electronically stored information is critical for healthcare providers. For example, a claim that an electronic medical record is “not reasonably accessible” is inconsistent

²⁶ *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003). *Zubulake* involves a series of decisions out of the Southern District of New York. See also *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). In *Zubulake*, the court was confronted with issues involving the discoverability of emails. The plaintiff requested email information which was claimed by the defendant to be “unavailable,” but the plaintiff had produced several hundred pages that demonstrated that the emails existed previously and based on the storage systems of the defendant should still be available.

²⁷ See *Zubulake v. UBS Warburg*, 217 F.R.D. at 319-20. The Court’s reasoning regarding accessibility was ultimately applied to the question of whether or not costs should be shifted to the requesting party. See Section 4, *infra*.



As leaders in the field of health law, HDJN attorneys offer a unique blend of experience, innovation, responsiveness and clear communication that is widely recognized for its effectiveness.

with the basic purpose of the electronic medical record.²⁸ However, in the scenario where legacy medical records which have been scanned into an electronic database, backed up, moved offsite, and based on proprietary no-longer-existent software, a claim that ESI is not reasonably accessible becomes plausible. Many healthcare providers, in an effort to stay ahead of the technological curve may already find themselves in this type of position. When planning for the expansion of electronic discovery in Virginia, healthcare providers and their technology support personnel are well advised to look at how much information is or will become unavailable when a facility upgrades computer systems. If such information is retrievable once the hardware or software is no longer in active use, the cost of such data mining efforts becomes a significant potential concern.

One temptation with the “reasonably accessible” requirement is the potential overly expansive application of that claim in an effort to avoid disclosing data that may not help the defense of the case. Expect this to be a battleground in pretrial discovery during medical malpractice cases. It is unlikely that Virginia courts will permit anything less than a forthright and articulate basis for a claim of not reasonably accessible. Ordinary electronic medical records are unlikely to be subject to any claim of “not reasonably accessible.” The healthcare provider’s duty to obtain and maintain certain health data arguably creates an affirmative obligation to maintain such data in an accessible format for an indefinite

amount of time, not less than the routine storage periods for traditional paper records.

But ESI also reaches far beyond electronic “medical records.” Healthcare providers will be confronted with other questions regarding electronic information that are equally as sensitive and may be subject to the same standard of “not reasonably accessible.” For example, a surgery case may involve a medical robotics device with its own electronically stored information. Anesthesia monitoring equipment may print out data at fixed intervals in the “electronic medical record,” but the computer may store vast amounts of additional data that never makes it to the record.

Ultimately, the healthcare provider will be required to prove that the information identified is not reasonably accessible. Whether this data is maintained, how this data is maintained, who controls this data, and how this data can be analyzed are critical questions. When electronic discovery requests are pursued in Virginia under the anticipated new rules, these questions will provide the framework for assessing whether or not this information is discoverable based on its “reasonable accessibility.”

3) Good Cause – When You Really Need It

Even if a party states that electronically stored information is not reasonably accessible and is able to make a sufficient showing to the Court, “the court may nonetheless order discovery from such sources if the requesting party shows good cause.” The Draft

²⁸ The U.S. Department of Health and Human Services has described the importance of electronic medical records, “The medical clipboard becomes a thing of the past. Secure, interoperable electronic records are available to patients and their doctors anytime, anywhere. Immediate access to accurate information reduces dangerous medical errors and helps control healthcare costs. This, in turn, establishes standards and ensures efficient collection of quality information.” CMS Strategic Action Plan 2006-2009, U.S. Department of Health and Human Services 12 (October 16, 2006) (available at http://www.cms.hhs.gov/MissionVisionGoals/Downloads/CMSStrategicActionPlan06-09_061023a.pdf).



HDJN offers legal solutions to handle the challenges of an ever-changing healthcare landscape.

ESI Rules do not provide a definition for “good cause,” particularly in the context of electronically stored information. When confronted with a claim that information is not reasonably accessible, the federal courts will provide some guidance.

For example, in *W.E. Aubuchon Co., Inc. v. Benefirst, LLC*, a federal magistrate was confronted with a discovery request involving the management of medical benefits and electronically stored medical claims files.²⁹ The electronic files at issue were scanned copies of paper claims which were later destroyed.

The electronic files were not organized in a manner that made retrieving information efficient. Benefirst argued that the files were not reasonably accessible because of the amount of time and financial expense of locating the information requested by the plaintiff. The court agreed that the information was not reasonably accessible because of the format of the electronic information. But the plaintiff claimed that good cause existed for the production of the electronic information and the court agreed with this position as well, granting access. Because the electronic information was the only source for the claims information and claims information was directly relevant to the case, Benefirst was required to produce the claims information requested in discovery at its own expense.³⁰

In healthcare, the circumstances are often such that the patient has inferior knowledge and lack of access to information which will perhaps sway the court’s analysis in favor of more expansive disclosure. For example, the patient may be a minor, may have

been under anesthesia during the critical time period, or may now be deceased. The sympathies of the case will often lie with the patient who had an unexpected and unfavorable outcome. Occasionally there are gaps in the official medical record – particularly in times of crisis. We can expect that plaintiffs will rely upon these equitable arguments to push for broad disclosure of electronic information.

4) Shifting the Cost For Not Reasonably Accessible

Even if a party demonstrates good cause, thus allowing access to not reasonably accessible information, “the court may specify conditions for the discovery, including allocation of the reasonable cost thereof.”³¹ Practically speaking, costs are an important consideration in civil litigation. In Virginia, a party subject to a discovery request is responsible for the costs of complying with that discovery request under ordinary circumstances. Reflecting the reality that electronic discovery can be particularly expensive, the Draft Rules now specifically provide for a cost shifting mechanism. Courts will now have the authority to require the requesting party to pay for any “fishing expeditions” into electronic information that is not reasonably accessible. The cost shifting provision may ultimately make unreasonable electronic discovery unattractive when the cost of accessing the information is weighed against the questionable value of the information.

Cost shifting, like the standard of “reasonably accessible,” is rooted in the *Zubulake* case. The seven factors the court considered there were: 1) the extent to which the request was

²⁹ *W.E. Aubuchon Co., Inc. v. Benefirst, LLC*, 245 F.R.D. 38 (D. Mass. 2007).

³⁰ Benefirst had claimed that the initial production requested by the plaintiff would have cost approximately \$80,000 and would have taken 4,000 hours to retrieve the information. The plaintiff narrowed the request from 34,112 claims to 3,000. No new cost analysis was provided by Benefirst.

³¹ See Draft ESI Rule 4:1(b)(7).



Our clients increasingly look to us for comprehensive legal assistance, and our aim is simple: as a business-oriented firm, we strive to develop practical solutions to our clients' legal needs in a timely and cost-effective manner.

narrowly tailored; 2) availability of the information from other sources; 3) total cost of production compared to the amount in controversy; 4) total cost of production compared to the resources of each party; 5) relative ability of each party to control costs and the incentive of each party to do so; 6) the importance of the issues in the litigation; and 7) the relative benefits to the parties of the information.³²

Recovery of electronic information can be expensive. And consideration of the seven factors may weigh against the shifting of costs when most medical malpractice litigation involves individuals versus healthcare providers. When confronted with the disparity in relative resources between parties, healthcare providers may be left to foot the bill. But that is no reason for healthcare providers to expect to pay the freight for any and every ESI request. Many ESI requests may come in the form of third party subpoenas; as a result, these requests may be more susceptible to cost shifting considerations. Risk managers and other healthcare professionals need to be prepared to determine how the cost of discovery integrates into the entire litigation strategy.

5) Safe Harbor for Stormy Seas

The Draft Virginia ESI Rules recognize the real world complexity of handling electronic information by providing for a safe harbor when electronic data is inadvertently destroyed, but this safe harbor provision may not provide complete protection. "Absent exceptional circumstance, a court should not impose sanctions upon a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."³³

This provision recognizes that vast amounts of relevant electronic

information can be destroyed or otherwise rendered unusable with a single keystroke or other unintended misadventure. And the rules would seem to provide for this contingency, but the protection may not be as robust as it would appear.

The Federal Rules have a similar provision providing for safe harbor. Federal courts have enforced this provision by examining the circumstances which resulted in the "lost" ESI. For example, in *Escobar v. City of Houston*, the plaintiff filed a wrongful death suit against the City of Houston involving a police shooting.³⁴ Within sixty days of the shooting, the plaintiff notified the City of the claim (hence, the City should have ensured that ESI that was relevant to the claim was preserved, just as with any other discoverable information).

During the course of discovery two years later, the plaintiff learned that the City had deleted all email correspondence pursuant to city policy that electronic communications were only kept for ninety days. The plaintiff sought sanctions for the destruction of this electronic correspondence in the form of an adverse-inference instruction. Although the court believed that the City was on notice of a claim by the plaintiff within sixty days of the incident and that the City had a duty to preserve the electronic correspondence, the court found that the safe harbor provision for destruction of electronic operation during routine system operation made sanctions inappropriate.

Despite the protections in the federal version of the safe harbor rule, safe harbor for the destruction of electronic evidence during routine system operation has not been guaranteed by federal courts and will likely not be

³² See *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003).

³³ Draft ESI Rule 4:12(e).

³⁴ *Escobar v. City of Houston*, 2007 U.S. Dist. LEXIS 72706 (S.D. Tex. Sept. 29, 2007).



In addition to representation of Virginia clients, the firm has attorneys licensed to practice law in most surrounding states, namely: Maryland, the District of Columbia, North Carolina, Tennessee and West Virginia. HDJN also has lawyers licensed to practice law in California, Georgia, Pennsylvania and New York.

guaranteed by state courts interpreting Virginia's similar provision. Where a party had notice that ESI may be at issue, safe harbor has not been an effective shield.

In *Doe v. Norwalk Community College*, the plaintiff alleged Title IX and state law claims of negligent retention and supervision and negligent infliction of emotional distress.³⁵ During litigation, the plaintiff requested sanctions for failure to preserve ESI, including emails from the time period involving the plaintiff's claim. Once the emails were produced, there were obvious gaps in the relevant email history that were inconsistent with the email retention policy of the facility.³⁶ Despite the safe harbor provision, the court found the defendant did not take the affirmative steps necessary to preserve ESI once litigation was reasonably anticipated; therefore, the court granted the plaintiff's request for an adverse inference instruction and monetary sanctions.

Courts have the inherent authority to provide for a wide range of sanctions for spoliation of evidence, and courts are serious about parties and their counsel complying with electronic discovery provisions. Earlier this year in *Qualcomm Inc. v. Broadcom Corp.*, a California federal district court granted a motion for sanctions for failing to produce electronically stored information - \$8.5 million dollars in sanctions against a corporation and referral of six attorneys for the corporation to the State Bar of California.³⁷ The sanctions were independent of the verdict. Although this ruling represents the exception rather than the rule in litigation involving electronic discovery issues, it

demonstrates that federal courts do not have any patience for parties or their counsel who do not faithfully conform to discovery requirements – particularly in light of specific rules highlighting procedures to be used in electronic discovery.

With the increased importance of ESI as a source of proof, sanctions for destruction or non-production of evidence (even unintended) are a distinct possibility. Penalties can vary from mere monetary penalty, like the \$8.5 million in *Qualcomm*, to adverse-inference instructions, like the sanction in *Norwalk Community College*, to the ultimate penalty of summary judgment (or dismissal with prejudice). Proper handling of electronic information is essential to avoid penalty by the courts.

Where to Go From Here

It is advisable for those who work to defend healthcare litigation in Virginia to prepare for the realities of electronic discovery. The plaintiff's bar will be prepared to leverage all aspects of electronic discovery. There are steps that healthcare providers can take to prepare to effectively handle electronic discovery requests from the medical malpractice context:

- 1) Survey the electronic information that your practice or facility currently uses, system wide;**
- 2) Survey the electronic information that is generated specifically in the healthcare environment;**
- 3) Know what information is controlled in-house and what is controlled by third parties;**

³⁵ *Doe v. Norwalk Cmty. College*, 2007 U.S. Dist. LEXIS 51084 (D. Conn. July 16, 2007).

³⁶ The defendant also claimed that emails could not be preserved under any policy because the "Jane Doe" status of the plaintiff would have been compromised. The court was nonplussed by this assertion, reminding counsel that parties can confer regarding reasonable solutions to discovery problems.

³⁷ See *Qualcomm Inc. v. Broadcom Corp.*, 2008 U.S. Dist. LEXIS 911 (S.D. Cal. 2008). This sanction represented the cost of the prevailing party's litigation. The key lesson from this ruling, failure to appropriately search for electronic files for information responsive to an opposing party's request can result in harsh penalties from the court.



The information contained in this advisory is for general educational purposes only. It is presented with the understanding that neither the author nor Hancock, Daniel, Johnson & Nagle, PC, is offering any legal or other professional services. Since the law in many areas is complex and can change rapidly, this information may not apply to a given factual situation and can become outdated. Individuals desiring legal advice should consult legal counsel for up-to-date and fact-specific advice. Under no circumstances will the author or Hancock, Daniel, Johnson & Nagle, PC be liable for any direct, indirect, or consequential damages resulting from the use of this material.

For more information about HDJN visit the firm website at:
www.hdjn.com

4) Ensure that systems are in place to preserve electronic data when necessary to avoid routine destruction;

5) When litigation is anticipated, start preserving electronic data; and

6) Get to know your IT staff and discuss with them the issue of electronic discovery in malpractice litigation.

Also consider identifying and using legal counsel to develop an electronic discovery blueprint and plan – **before** you find yourself in the midst of a discovery battle in an ongoing case. Given the specialized nature of the healthcare industry, utilize a law firm that has the resources to understand how federal and state statutory and

regulatory requirements can impact the storage, retrieval, and dissemination of electronic health information. Specialized medical malpractice experience will further complement the development of an electronic discovery plan that leverages the guidelines established by federal and state rules of civil procedure.

Hancock, Daniel, Johnson & Nagle, P.C., has the full spectrum of resources to address every angle of electronic discovery in the healthcare industry. Please feel free to contact the authors (Sean P. Byrne or Neal H. Lewis) at (804) 967-9604 or by email (sbyrne@hdjn.com or nlewis@hdjn.com) if you have any additional questions.

About the Authors

Sean P. Byrne – Sean Byrne is a Director in the firm practicing in the area of civil litigation. He primarily represents hospitals, physicians, and other healthcare providers and institutions in the defense of medical malpractice lawsuits, and by providing healthcare risk management education and advice. Mr. Byrne has represented and counseled healthcare providers in responding to electronic discovery requests. He is a Virginia Certified Emergency Medical Technician and is very familiar with the technology used in the provision of patient care.

Neal H. Lewis – Neal Lewis is an Associate in the firm's civil litigation section. His practice concentration is civil litigation, including medical malpractice defense, employment law, and general commercial litigation. Mr. Lewis has been extensively involved with technology issues serving as Editor-in-Chief of the Richmond Journal of Law & Technology and authoring several articles regarding the issues involved with electronic discovery. He has been certified in computer hardware (A+), networking systems (Network+), and as a Microsoft Certified Systems Engineer.

<p>Richmond 4701 Cox Road, Suite 400 Glen Allen, VA 23060 PO Box 72050 Richmond, VA 23255-2050 ☎ (804) 967-9604</p>	<p>Fairfax 3975 Fair Ridge Road Suite 475 South Fairfax, VA 22033 ☎ (703) 591-3440</p>
<p>Harrisonburg 3210 Peoples Drive Harrisonburg, VA 22801 ☎ (866) 967-9604</p>	<p>Virginia Beach One Columbus Center 283 Constitution Drive Suite 301 Virginia Beach, VA 23462 ☎ (757) 321-6555</p>

HANCOCK, DANIEL, JOHNSON & NAGLE, P.C.