THE E-DISCOVERY RULES:
PRACTICAL APPLICATIONS FOR RISK MANAGERS

By: Christopher J. Allman, J.D. and A. Tony Taweel, J.D.

Introduction

On December 1, 2006, amendments were implemented to the Federal Rules of Civil Procedure[1] (the "Rules") regarding electronic discovery ("e-discovery"). These rules effect how health care providers manage their electronically stored information. More importantly, these rules directly impact how a risk/claims manager must respond to discovery requests.

It is now imperative to evaluate existing policies and procedures related to record retention and electronically stored information and implement a process to ensure access to and preservation of electronic information, data, and records which may be subject to litigation[2]. Failure to comply with these rules has negative impacts, which could include sanctions, the opposing party receiving the benefit of the doubt on the subject matter of the missing evidence, and, potentially, criminal charges.

What is "Electronic" Discovery?

Electronic Discovery includes any organization's Electronically Stored Information ("ESI")[3]. The Federal Rules on electronic discovery address the form of production of ESI, whether information is accessible or not reasonably accessible, and sanctions for failure to produce ESI when required to do so[4].

What Do the E-Discovery Rules Do?

The e-discovery rules impose a duty to preserve ESI when a legal complaint is filed, where a party reasonably anticipates that litigation is likely to commence or once it receives a discovery request during litigation[5]. Anyone who anticipates being or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary. A litigant is under no duty to keep or retain all ESI in its possession but is under a duty to preserve ESI that is relevant to the subject matter involved in the case or supports the claims or defenses of any party. This duty extends to those employees who

---

[1] The Federal Rules of Civil Procedure govern procedure for all civil suits commenced in United States District Courts. The Rules are established by the United States Supreme Court and approved by Congress.

[2] While this article focuses on the federal rules, E-discovery rules have been adopted by most states. Most states' rules are similar to the federal rules, but they may contain differences particular to your locality. It is therefore important to know whether your state has adopted such rules, and, if so, what these rules specifically require.

[3] ESI may include, but is not limited to: e-mails, spreadsheets, WordPerfect files, text messages, data from PDAs, internet use histories, files downloaded from the internet and offline storage archives, Electronic Health Records (EHRs typically include records from laboratory information systems, pharmacy information systems, picture archives of communication systems, results reporting systems and computerized provider order forms.). See F.R.C.P. Rule 34(a)(1)(A)

[4] See F.R.C.P. Rules 34 and 37

[5] F.R.C.P. Rule 34(a)

are likely to have relevant information and the "key players" in the case. This duty remains in effect as long as a party should reasonably foresee that further evidence material to a potential civil action could be derived from this evidence.[6]

There are exceptions, however. The Rules state "absent exceptional circumstances, a court may not impose sanctions under these rules on a party failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system.[7]" However, the Rules go on to say that "the good faith requirement means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing the operation to continue in order to destroy specific stored information that it is required to preserve." Any policy or procedure must therefore mandate the suspension of ordinary destruction practices and procedures.

How Do We Produce ESI?

The requesting party may specify the form in which it would like for ESI to be produced[8]. If no form is specified ESI may be produced in a form ordinarily maintained or in a form reasonably useable[9]. Most importantly, a request may be made for electronic discovery in its native format, which includes "metadata"[10].

Considerations for ESI Collection When Litigation is Anticipated or Commenced

- Contact the IT department and identify the location of all relevant information
- Identify who the key players are and units/departments that have information relevant to the claims or defenses of any party
- Consider all potential timeframes and documents involved
- Designate the custodian of all relevant data[11]
- Consult legal counsel to determine whether an amended litigation hold should be issued

Risk Management Recommendations

1. **Develop a multidisciplinary committee** to review existing policies and procedures for record retention, destruction of documents (paper or electronic), and automatic destruction or purging of ESI in light of the e-discovery rules. The committee should also develop a comprehensive list of IT systems and cross

---

[6] *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("Zubulake I")
[7] F.R.C.P. Rule 37(e)
[8] F.R.C.P. Rule 34
[9] *Id.*
[10] The native form of a document contains related background information that may not be visible in print known as "metadata." Common metadata includes: the date and time of the last modification, the author's name, the date the document was created, along with comments/annotations of the document, edit dates and users having access to the document.
[11] See F.R.C.P. Rule 30(b)(6)

reference the type and location of electronic data stored. Suggested individuals may include:

- Risk Management
- Information Technology
- Health Information Services
- Privacy Officer
- Information Security Officer
- Patient Relations
- Legal Counsel

2. **Identify existing policies and procedures** pertaining to electronic health records, e-mail, personnel records, business records, or any other type of document stored electronically; identify policies and procedures for record retention, record destruction and electronic records management, and providing materials in response to subpoena, court order, or request from an attorney related to litigation. These policies should be reviewed for adequacy and identify gaps and issues related to e-discovery.

3. **Develop a "Litigation Reaction Plan"** For developing and implementing policies and procedures that address:

   - Dissemination of the "litigation hold letter" received from legal counsel to key employees who have access to the requested information;
   - Suspension of document destruction;
   - Removal of back-up tapes from the normal rotation of destruction; and
   - Engaging consultants, particularly if necessary to obtain information forensically.

4. **Develop a comprehensive communication and education program** to educate all members of the health care facility about the existence of the ESI policies and procedures to follow if a claim is filed.

5. **Designate an individual who, if needed, could testify about your organization's retention policies, procedures, storage and record security.** If testimony is required regarding any issues surrounding your organization's ESI, designating one knowledgeable individual to provide this information will result in consistent testimony of these policies by a knowledgeable individual.

Conclusion

The Rules regarding discovery of electronic information affect how all health care providers manage the destruction or preservation of electronically stored information. Therefore, when events occur which are reasonably anticipated to result in litigation, or litigation has commenced, documents stored in an electronic form must be preserved. Furthermore, if your organization becomes party to a lawsuit, communicate this

information to key leadership in the organization immediately and suspend destruction of electronically stored information. Finally, contact legal counsel immediately to assist your organization with preservation of evidence matters.

About the Authors

Christopher J. Allman, J.D. and A. Tony Taweel, J.D. are principals in the law firm Ottenwess, Allman & Taweel, PLC in Detroit, Michigan. Their firm specializes in healthcare law and litigation and medical malpractice defense. Chris is also currently President-Elect of the Michigan Society for Healthcare Risk Management.