IADC Committee Newsletter

DRUG, DEVICE AND BIOTECHNOLOGY

June 2011

IN THIS ISSUE

E-discovery sanctions are increasing each year. In order to be prepared for e-discovery requests and sanctions motions, you must aggressively and proactively start preparing your clients with an e-discovery readiness plan, long before a lawsuit has even been filed. This article discusses some necessary basic steps in this process.

Defending Against E-Discovery Sanctions Begins Yesterday

ABOUT THE AUTHOR

Jeffrey Lilly is a Partner in Gordon & Rees's Houston and Austin offices and is a member of the firm's Drug & Medical Device practice group. His diverse practice includes representing a broad range of clients in product liability, toxic tort and commercial litigation matters in state and federal courts, including national MDLs. He has a special interest in e-discovery.

ABOUT THE COMMITTEE

The Drug, Device and Biotechnology Committee serves as an educational and networking resource for in-house counsel employed by pharmaceutical, medical device and biotech manufacturers and the outside counsel who serve those companies. The Committee is active in sponsoring major CLE programs at the Annual and Midyear Meetings as well as internal committee programs. The Committee also publishes a monthly newsletter that addresses recent developments and normally contributes two or more articles to the *Defense Counsel Journal* annually. In the future, the Drug, Device and Biotechnology Committee will be focusing on increasing its use of technology to make it an even more valuable resource for its members.

Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Eric M. Anielak
Interim Vice Chair of Publications
Shook, Hardy & Bacon, L.L.P.
(816) 474-6550
eanielak@shb.com

I. Introduction

Defending against e-discovery sanctions begins long before the start of a litigation hold. No matter how big or small a business, volumes of electronic data are generated every minute of every day. Consider the many and different forms of electronically stored information (ESI) in most any company — e-mails, voice-mails, videos, internet searches, social media activity, back-up tapes, clouds, smart-phone generated data, etc. While with paper files you could (and still can) wait for a litigation hold to be imminent before taking action to consider how to preserve potentially discoverable information, in this digital age information is stored and, more relevant for e-discovery purposes, deleted without a human finger being lifted and with no regard for what may or may not be discoverable for a later lawsuit.

Are you prepared to avoid sanctions for e-discovery abuse? Do you have a well conceived written plan for protecting future discoverable data from being auto-deleted as soon as a litigation hold is in place? Considering how to preserve electronic information *after* a litigation hold may be too late. If you are not aggressively and proactively preparing a well thought out plan to preserve ESI on a moment's notice, you are at risk for losing discoverable data and, with each day that goes by, potentially costly and/or damaging motions for sanctions as well.

II. Background

A recent white paper on e-discovery issues calls 2010 "the year of the sanctions" and predicts that 2011 will "continue to be dominated by motions for sanctions for alleged preservation failures."[1] Likewise, a comprehensive study on e-discovery sanctions shows increases in e-discovery sanctions motions as well as awards every year since the 2006 amendments to the Federal Rules of Civil Procedure addressed ESI.[2] Sanctions for e-discovery abuse cover a broad spectrum, including damaging adverse inference instructions[3] and monetary penalties ranging from as little as $250 to as high as $8,830,983.694.[4] There is no consensus as to what the standard should be for imposing e-discovery sanctions — some courts have imposed sanctions based on mere negligence or gross negligence, while others have required bad faith. Under any standard, good intentions with detailed protocols that are consistently followed will bolster a defense against sanctions, so caution is the better part of valor; effort should be made to remove any colorable argument that there was anything other than a good faith attempt to be prepared for and, in fact, to preserve appropriate ESI.

---

[1] Hon. A. Peck and D. Lender, "Ten Key E-Discovery Issues to Watch in 2011: Expert Insight to Manage Successfully", p. 6 (Huron Consulting Group, Inc., 2011).

[2] *See* Willoughby, Dan H., Jones, Rose Hunter and Antine, Gregory R. *Sanctions for EDiscovery Violations: By the Numbers*, Duke L.J. 795, Vol 60: 789.

[3] Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598 (S.D. Tex. 2010).

[4] *See* Willoughby, Dan H., Jones, Rose Hunter and Antine, Gregory R. *Sanctions for EDiscovery Violations: By the Numbers*, Duke L.J. 861-864, Vol 60: 789.

III. Necessary Pre-Litigation Hold Steps to Reduce Risk of Later E-Discovery Sanctions

A. Investigate and Analyze Internal Electronic Systems

As a routine business practice, companies must fully understand their systems, including their capabilities and limitations, and reduce their knowledge to a user friendly internal manual for reference. (Never has a top notch Information Technology employee with an understanding of litigation been so valuable.) Don't wait for a lawsuit to begin to try to grasp the totality of ESI, where and how it is stored (create a data map), who is the most knowledgeable person internally for each system, and how each system can be modified — primarily deletion, preservation, and search capabilities.

This can be a massive and tedious process even with the luxury of time, which you will not have if a lawsuit is approaching. There are many questions to answer, including by way of example only: 1) How many different forms of ESI exist and where are they?; 2) Who has access to them?; 3) How long are the various forms of ESI customarily stored?; 4) How and when is the ESI deleted?; 5) Are back-up systems in place and where?; 6) Do employees store information on personal devices?

Other important factors for later consideration are whether any information is stored with a third party, such as with a vendor or in a cloud. (Ideally, as storage with third parties impacts later discovery and privilege issues, this was already considered in deciding modes and locations of information storage, but that is a lengthy topic for another article.)

B. Develop a Comprehensive Plan for Day to Day handling of E-information

After you have a thorough understanding of the universe of electronic information that exists, how and where it is stored, and who has the internal expertise to assist, the next step is to establish a clear protocol for managing each system both day to day under normal business operations, but more importantly when a change in customary preservation processes becomes necessary in response to a litigation hold.

C. Audit Your Auto-Deletion Systems

To protect from claims that a systematic and pre-determined deletion schedule was only in theory, make sure that the auto-deletion schedule is in fact working as designed. In other words, if you have e-mail set to delete and disappear within 120 days, check repeatedly (and document that you have done so) to see if the deletions are occurring on schedule.

This is critical to fending off sanctions at a later date, as any accusation that pre litigation hold information has been improperly discarded will need to be met with the fact that such information was deleted in the ordinary course of business as part of a pre-established plan, and *not* in response to any issues arguably related to the case. Importantly, however, this plan must include detailed protocols for how to suspend the auto-deletion as soon as a litigation hold is in place.

D. Conduct Periodic E-Discovery Fire Drills

No matter how comprehensive e-discovery plans and protocols are, they will only protect from sanctions if they can be successfully executed emergently. Simultaneous with

issuing a litigation hold, the systems for making sure information is preserved need to be initiated so that not even one byte of potentially discoverable information is lost. The best way to do this is to run periodic and unannounced fire drills to see if auto-deletions of information can be deftly suspended, so that more careful thought can be given to what specific parameters should be set for preservation of the precise information that will need to be retained in response to the litigation hold.

E. Stay Abreast of E-Discovery Law and Related Technology

Chances are an e-discovery plan will be outdated the moment it is finalized. To stay protected against future sanctions claims, individuals will need to be designated to: 1) stay up to date on developments in e-discovery law and sanctionable activities; and 2) stay knowledgeable on any changes in internal technologies.

IV. Conclusion

Defendants are sanctioned three times as often as plaintiffs and the most common reason for sanctions is failure to preserve information.[5] Avoiding being sanctioned for e-discovery abuse *is* doable, but requires a well thought out plan far in advance of any future litigation hold. The very nature of the planning will be the best evidence of an intention to make certain electronic information was responsibly managed. Without this record of activity, defending against a motion for sanctions will be more difficult if some information is lost, even inadvertently.

[5] "Sanctions for E-Discovery Violations: By the Numbers," by Dan H. Willoughby, Jr., Rose Hunter Jones, and Gregory R. Antine. P. 803, Duke Law Journal, Vol 60: 789.

PAST COMMITTEE NEWSLETTERS

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

APRIL 2010
Managing Risks Associated with Off-Label Promotion of Pharmaceuticals
Michael F. Healy and Kelly Savage Day

FEBRUARY 2010
Name-Brand Manufacturers Liable for Ingestion of Generic Products?: An Analysis of The Nation's Response to California's *Conte v. Wyeth* Decision
Jack B. McCowan, Jr., Kai Peters and Stephen Lawniczak

DECEMBER 2009
Medtronic Class Actions in Canada – Important Developments for Manufacturers: Ontario Court Provides Relief from Burdens of Disgorgement and Punitive Damage Claims
S. Gordon McKee, Robin Linley, Karin McCaig and Nicole Henderson

NOVEMBER 2009
The Applicability of *Twombly* & *Iqbal* to Pharmaceutical Product Liability Litigation
Archie Reeves

OCTOBER 2009
Wyeth V. Levine, Six Months Later – What Remains of Prescription Drug Preemption?
By Dabney Carr and Brian Fowler

AUGUST 2009
Australia's Move towards Harmonised Consumer Laws: Unintended Effects for Drug and Medical Device Manufacturers
Dr. Jocelyn Kellam, Larissa Cook, and Stuart Clark

JUNE 2009
Drug Diversion and Counterfeiting – A Decades-Old Problem Remains Unsolved
Kathleen H. Dooley

MAY 2009
Strategies for Defending the Fraudulent Joinder of Sales Representatives in Pharmaceutical and Medical Device Litigation
Lori G. Cohen and John B. Merchant, III

MARCH 2009
Rx for the Times?
Leta Gorman