E-Health, Privacy, *and* Security Law

Third Edition

Editor-in-Chief

W. Andrew H. Gantt III
Cooley LLP
Washington, D.C.

Chapter 18
Legal Ethics and E-Health

Sheryl T. Dacso / *Seyfarth Shaw LLP*
Kari K. Loeser / *Genentech, Inc.*

AMERICAN BAR ASSOCIATION
Health Law Section

The American Bar Association
Health Law Section

Bloomberg BNA

Bloomberg BNA, Arlington, VA

Published by Bloomberg BNA
1801 S. Bell Street, Arlington, VA 22202
bna.com/bnabooks

ISBN 978-1-68267-009-5
Printed in the United States of America

18

Legal Ethics and E-Health*

*Sheryl Tatar Dacso, J.D., Dr. P.H., Seyfarth Shaw, LLP, Houston, Texas; Kari Loeser, J.D., Jazz Pharmaceuticals, Palo Alto, California.

I. Introduction

The Internet, combined with growing technology capabilities, offers unprecedented access to information, products, and services. At the same time, it makes possible forms of communication and practices that raise ethical and legal concerns. Relationships between attorneys and their clients as well as entire transactions can occur without a face-to-face encounter. The availability of social media presents opportunities for marketing but heightens liability exposure for inadvertent disclosures and implied attorney-client relationships.

New challenges continue to arise associated with the increased use of the Internet, computers, and mobile devices, which have become a ubiquitous means of communication between attorneys and their health care clients as well as among attorneys concerning their health care clients and among the health care clients themselves. Recent developments with the use of "ransomware" by criminals, both domestic and foreign, presents serious problems for hospitals and other health care providers who face the difficult decision of paying a ransom to regain their ability to operate or risk patient safety and compliance. Law firms face similar vulnerabilities with increased reliance on internet storage of client files containing confidential financial, intellectual property and personal information. The "internet of things" and increased reliance on technology makes cyber-security protection a necessity for those who rely on internet-based technology, whether it is "in the cloud" or on a server. These changes in technology, coupled with the increased use of social media and the handling of online criticism raise legal and ethical issues for health lawyers and their clients.[1] There is no better example of how dependent we are on computer technology and the Internet than a disaster (including being cut off from access and use of computer-based information via cybercrime), which can seriously disrupt and potentially destroy important client information, and which poses a legal and ethical obligation to prepare for disasters, including the ability to secure, preserve and recover electronic information.[2]

The pervasiveness of information technology raises complex and new approaches to the analysis of an attorney's legal duty and ethical responsibility. This chapter first discusses the use of information technology by health care lawyers and the effect of such technology on the attorney's ethical responsibilities and legal duties to his or her client. It next addresses new areas of liability, as the expanding use of technology intersects with legal ethics rules with respect

[1]See Section II.B.2., below.

[2]See Section II.A.2.f.ii., below.

to matters of attorney competence in its use and deployment in practice, as well as heightened compliance obligations with respect to client information privacy and confidentiality. This includes issues related to the use and storage of information that may be subject to civil and criminal investigations or client misconduct and e-discovery issues. The last part of the chapter considers several complex and difficult conflict-of-interest issues that may confront the health care practitioner who, on one hand, maintains a privileged attorney-client relationship with his or her client but, on the other hand, because of that relationship assumes separate legal duties for maintaining the privacy and security of protected health information and complying with federal and state laws, rules, and regulations.

The legal system and ethical guidelines often lag behind technology, so attorneys who work with clients that use health information technology and who use such technology themselves must constantly stay informed of both ethical and legal duties. Although the list of issues is not exhaustive, those discussed in this chapter are the ones currently posing important concerns for the conscientious lawyer.

Attorneys who use mobile devices to communicate sensitive information by text appearing to come from colleagues need to take special precautions. For example, hackers looking for insider trading information may target attorneys involved in mergers and acquisitions and put links in text messages that can activate malware to log the keystrokes and phone conversations. As cyberattacks against law firms increase, attorneys must be increasingly vigilant in using secure systems to communicate sensitive client information. For this reason, many bar associations are suggesting that attorneys take technological steps to protect client information as part of their ethical duties.

The American Bar Association (ABA) and states' ethics rules impose duties on attorneys to protect client confidences. They also require attorneys to practice competently and to supervise office staff and third parties who are given access to client data. These rules will require attorneys and law firms to implement reasonable information security practices to protect the confidentiality, integrity, and availability of client data. Failure to protect client data may lead to attorney discipline or even malpractice liability. Information security is not just a "technology issue" that can be delegated without supervision to information technology support staff. Attorneys themselves have an obligation to manage and oversee the security function in their firms. Lessons learned from other industries and industry standard security frameworks can help law firms implement effective security programs.

In May 2012, the ABA Commission on Ethics 20/20 submitted to the ABA House a Resolution and Report on Technology and Confidentiality that are intended as a guide to lawyers regarding the use of technology. These were proposed and approved as amendments to the Model Rules of Professional Conduct and changed Model Rules 1.6 (Confidentiality of Information) and 1.1 (Competence) in August 2012. Model Rule 1.6, Comment [16], was rewritten to include factors to be considered in determining the reasonableness of a lawyer's efforts to prevent disclosure or access. For example, a lawyer should make reasonable efforts to prevent disclosures or access, such as avoiding a lawyer's sending an e-mail to the wrong person, someone's "hacking" into a law firm's

Also available as part of the eCourse
2017 Health Law eConference

First appeared as part of the conference materials for the
29th Annual Health Law Conference session
"Telehealth: Tackling Technology's Legal and Ethical Impact on Healthcare"