IADC COMMITTEE NEWSLETTER

# MEDICAL DEFENSE AND HEALTH LAW

*MARCH 2015*

### IN THIS ISSUE

*Robert G. Smith outlines HIPAA security considerations in relation to electronic communications between healthcare providers and their patients.*

# Electronic Communications Containing Protected Health Information

### ABOUT THE AUTHOR

**Robert G. Smith** is a member/owner of the firm Lorance & Thompson, PC in Houston, Texas. Rob is a member of the Product Liability, Business Litigation, and Medical Defense & Health Law Committees of the International Association of Defense Counsel. He is on the steering committee for the ALFA International Product Liability & Complex Tort Practice Group. Rob's clients include physicians, hospitals, nursing homes, and manufacturers, among others. He has tried a wide variety of cases during his 20 years of practice. He can be reached at rgs@lorancethompson.com.

### ABOUT THE COMMITTEE

The Medical Defense and Health Law Committee serves all members who represent physicians, hospitals and other healthcare providers and entities in medical malpractice actions. The Committee recently added a subcommittee for nursing home defense. Committee members publish monthly newsletters and *Journal* articles and present educational seminars for the IADC membership at large. Members also regularly present committee meeting seminars on matters of current interest, which includes open discussion and input from members at the meeting. Committee members share and exchange information regarding experts, new plaintiff theories, discovery issues and strategy at meetings and via newsletters and e-mail.

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

**Mark Hansen**
**Vice Chair of Publications**
Heyl, Royster, Voelker & Allen
mhansen@heylroyster.com

Most information in the world today is created, transmitted, and stored electronically. Protected Health Information (PHI) is no different, and healthcare providers will use and be responsible for maintaining more electronic Protected Health Information (e-PHI) in the future, particularly as the use of electronic medical records becomes more ubiquitous.

Email, text messaging, and even video or audio files, are tools physicians and other healthcare providers can use to provide treatment recommendations and communicate with each other and with their patients. There are many possible benefits including:

1) Increase efficiency and productivity by reducing the number of phone calls back and forth;
2) Reduce administrative costs associated with staff making phone calls;
3) Reduce paper use and storage requirements for hard copies;
4) Reduce costs by eliminating additional office visits;
5) Patient information can be updated, providing additional detail to patients or updating physicians with a patient's condition, without an additional office visit and associated expense;
6) Increase patient satisfaction by reducing additional trips to the office or hospital; and
7) Exchange information between healthcare provider and patients on their own schedules rather than during only during office hours.

If a physician provides medical advice to a patient through electronic means it can create a doctor-patient relationship, and should not be used with new patients. While healthcare providers often use electronic tools to follow up with an existing patient, electronic communications should not be used with new patients or when diagnosing or treating new conditions.

Healthcare providers should provide accurate information through electronic communications, because material often becomes part of the patient's medical file and the patient may act on the information. It should be accurate because these communications may be used by other healthcare providers and may become exhibits in subsequent litigation. Healthcare providers should not use electronic communications to address medical emergencies or acute conditions, and patients should be instructed to go to the emergency room or come to the office as appropriate.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created rules for privacy and security of PHI. The Health Information Technology for Economic and Clinical Health Act (HITECH) went into effect in 2010, updating the HIPAA rules with increased penalties (the maximum penalty is now well over $1 million). The Omnibus Rule was announced in 2013, and further enhances protections for patients' privacy. Nevertheless, it is important to keep in mind that HIPAA does not specifically prohibit the electronic submission of PHI. To the contrary, the statute allows flexibility so that covered

entities and business associates can use "any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications" as required. *See* 45 CFR §164.306 (b). To that end, controls for devices must be considered including the disposal of e-PHI and the hardware or electronic media on which it is stored, formatting media for reuse, accountability for hardware and electronic media, as well as backup and storage. *See* 45 CFR §164.310 (d).

Physical safeguards include requiring personnel to use company owned devices that contain PHI only at the office and forbid personnel from taking them offsite. Covered entities can install user identification software or tags on devices, and enable remote formatting software.

A covered entity or business associate must consider technical safeguards such as:

1) Policies and procedures to allow access only to people or software that have been granted access;
2) User specific log-in information and tracking ability;
3) Procedures for accessing e-PHI during an emergency;
4) Procedures that automatically log off users after a certain period of inactivity;
5) Implement encryption of e-PHI;
6) Procedures that record or examine activity in information systems that contain e-PHI;
7) Mechanisms to confirm e-PHI has not been altered or destroyed unless authorized;
8) Procedures to authenticate the person accessing e-PHI; and
9) Procedures to confirm or to protect against unauthorized electronic transmittal of e-PHI.

*See* 45 CFR §164.312.

Technical safeguards can also include installing encryption software, using firewalls for devices that access the internet, installing antivirus software on devices, backing up data in multiple locations, biometric authentication such as fingerprint or retina identification, and ensuring the hardware and software is kept up to date.

Covered entities must develop procedures to preserve PHI transmitted electronically in the patient's medical record if the communication includes PHI. HIPAA requires PHI to be maintained for at least six (6) years, so emails between a physician and a patient that contain e-PHI must be backed up for at least six (6) years as well.

Electronic messaging can include any system that allows a covered entity and a patient or business associate to create, send, respond to, download, view, read, or otherwise manipulate information that could be PHI through email, text messaging, or video and audio clips. Many of these messaging systems may not yet be integrated into a healthcare provider's electronic medical record software package, and must be considered on an individual basis. As types of electronic communication and devices evolve, HIPAA security issues must be reconsidered and healthcare providers' procedures must evolve as well. The American Medical Association issued Code of Medical Ethics Opinion 5.026

discussing email and it instructs that email should not be used to establish a doctor patient relationship, a physician has the same ethical responsibilities to their patient as an in person encounter, patient should be given notice of potential breaches in privacy or confidentiality, and seek the patient's agreement in advance to communicate electronically before PHI is transmitted.

Before communicating with a patient through electronic channels, healthcare providers must give notice to their patients. Individuals have the right to request a covered healthcare provider to communicate through an alternative method. Covered entities must allow patients to request that PHI be communicated through an alternative means or at an alternative location. *See* 45 CFR §164.522 (b).

When healthcare providers consider the hardware and mobile devices they may use to communicate e-PHI with patients, they must consider that the information may be stored on the device itself, the server in their office, the telecommunications companies' servers, a website host server, or other locations that must be accounted for in light of HIPAA's security requirements. Although HIPAA does not limit healthcare providers to a particular device or channel of electronic communication, certain devices and communication channels are more secure than others.

Covered entities must consider what PHI their organization creates, stores, sends and receives and where the vulnerabilities are in the chain of electronic communication. For example, text messages generally are not encrypted. Ongoing risk analysis is necessary to assist healthcare providers in reducing their risk of disclosing confidential PHI and exposing them to lawsuits and penalties for compromised data.

A smart phone can be used for email and texting, but they are easy to lose, such as forgetting them in a coffee shop or at an airport security check point. You must consider how secure the device is or whether data could be accessed by someone who found the phone. Laptops and tablet devices are frequently lost and stolen, and can lead to a data breach.

Compliance with PHI security requirements is not one decision at the time a device or software is purchased, but is an ongoing process that must account for the physical, technical, procedural, personnel, and personal functions and abilities, particular in today's world where technology changes so quickly.

Healthcare providers and the attorneys who work with them should stay up to date on the regulatory duties and how new technology may impact how healthcare is delivered, because the provision of healthcare through electronic communication continues to become more prevalent.

**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:

FEBRUARY 2015
The False Claims Act Yesterday and Today
Stuart Miller and Jane Duke

JANUARY 2015
The Risks of Long Term Use of Narcotics for Pain Management: Preparing an Effective Cross Examination of the Over Prescriber
R. Douglas Vaughn and Sharrolyn Jackson Miles

NOVEMBER 2014
Recovery of Extraordinary Expenses Permitted in Wrongful Pregnancy Action
Mark D. Hansen and Emily J. Perkins

OCTOBER 2014
Illinois Court Issues Harsh Reminder that Physicians Must Supplement Prior Deposition Testimony with Any New Opinions before Trial
Mark D. Hansen and Melissa N. Schoenbein

SEPTEMBER 2014
Illinois Appellate Court Discusses Whether Applications for Medical Staff Privileges are Privileged from Production in Discovery
Mark D. Hansen and J. Matthew Thompson

JULY 2014
Illinois Supreme Court Rules Against Emergency Room Physicians in Resolving Split Among Appellate Districts Regarding Interpretation of Good Samaritan Act
Mark D. Hansen and J. Matthew Thompson

JUNE 2014
The Florida Supreme Court Rejects Caps on Noneconomic Damages in Wrongful Death Medical Malpractice Cases
Jeptha "Jep" F. Barbour and Jill F. Bechtold

MAY 2014
Requirement to Report Suspected Crimes in Long Term Care Facilities
Monica Frois and Stephanie Murphy

APRIL 2014
Drafting a Consent to Treatment? Defending an Apparent Agency Claim? Consider the Illinois Third District Appellate Court's Decision in *Steele v. Provena Hospitals*
Mark D. Hansen and J. Matthew Thompson

MARCH 2014
Arizona Court of Appeals Upholds Medicare Advantage Right to Recover Conditional Payments
Mary G. Pryor