by Rachel V. Rose, J.D., MBA

Transporting Protected Health Information in the Digital Age

What does it mean to "transport" something? According to the dictionary, it means "to carry, move, or convey from one place to another."[1] In the electronic world we live in and—as lawyers—in the reality that we practice and advise clients in, one issue that is continually on the forefront of discussion topics is transporting protected health information (PHI).[2]

As Microsoft founder Bill Gates stated, "We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next 10. Don't let yourself be lulled into inaction." Nowhere is this statement more apropos than in transporting PHI because of the increasing reliance on electronic health records and other forms of electronic media. Therefore, the purpose of this article is to provide attorneys with a semblance of the background of the relevant laws and who is impacted, as well as measures that can be taken to mitigate the risk of liability.

Legal Background

To appreciate the context of the following laws, it is first important to understand the relationship between electronic media and PHI. Specifically, electronic media means: (1) electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; and (2) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet; leased lines; dial-up lines; private networks; and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.[3]

Many of these devices and services are utilized to transport PHI from one entity to another. And, therein lies the liability.

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA).[4] The Privacy Rule and Security Rule followed. These were promulgated by the U.S. Department of Health and Human Services (HHS) in 2002 and 2003, respectively. Nearly 13 years after HIPAA became law, the Health Information Technology for Economic and Clinical Health Act (HITECH Act)[5] was enacted, and subsequent interim rules and the 2013 Final Omnibus Rule[6] followed. These three laws alone permeate every industry, whether in terms of health insurance portability or the creation, receipt, transmission, or maintenance of PHI.

These three laws define three main categories: covered entities, business associates, and subcontractors, which are defined as: (1) Covered Entity—a health care provider who transmits any health information electronically in connection with certain transactions, health plans, and health clearinghouses;[7] (2) Business Associate—a person who "creates, receives, maintains, or transmits" protected health information;[8] and (3) Subcontractor—a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate. This definition applies to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate agreement.[9]

Covered entities and business associates use both domestic and foreign entities to perform services involving PHI. Those companies or individuals that contract with business associates are referred to as subcontractors. Initially, express liability only applied to covered entities while it was implied for business associates and subcontractors. The July 14, 2010, Proposed Rules[10] and the Final Omnibus Rule expressly extended liability to business associates and their subcontractors.

Attorneys should also consider state and international laws as well. In Texas, a business associate and a subcontractor are actually considered a "covered entity," which is defined as, "any person who: (A) for commercial, financial, or professional gain, monetary fees,

Rachel V. Rose, J.D., MBA, is the co-author of the American Bar Association's "What Are International HIPAA Considerations?" *Rose is licensed in Texas and is the chair of the Federal Bar Association's Corporate and Association Counsel Division and vice-chair of the American Bar Association's Health Law Section Distance Learning Committee.* *© 2015 Rachel V. Rose. All rights reserved.*

or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site; (B) comes into possession of protected health information; (C) obtains or stores protected health information under this chapter; or (D) is an employee, agent, or contractor of a person described by Paragraph (A), (B), or (C) insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits protected health information."[11] This distinction can become important if both federal HIPAA and state HIPAA are implicated in either a domestic or international situation.

Preventive Measures

In April 2014, the Federal Bureau of Investigation (FBI) released a notification, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain."[12] Compliance areas were the focus, in light of the increase in the black-market sales of protected health information obtained from electronic health records (EHRs). As if the black-market sale of PHI was not enough, two notable reports provide additional reasons:

- According to a Ponemon Institute report dated March 2013, 63% of the health care organizations surveyed reported a data breach in the past two years with an average monetary loss of $2.4 million per data breach. The majority of each data breach resulted in the theft of information assets. Lastly, 45% reported that their organizations have not implemented security measures to protect patient information."[13]
- "A SANS report dated February 2014 indicates health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property. Data analysis revealed multiple devices (e.g., radiology imaging software, digital video systems, faxes, printers) and security application systems (e.g., Virtual Private Networks ("VPN"), firewalls, and routers) were compromised. Once medical devices are compromised, malicious traffic is transmitted through VPNs and firewalls. The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise."[14]

These two reports illustrate that the potential liabilities for noncompliance with HIPAA and related laws and regulation are vast. Therefore, how PHI is transported is crucial.

Now that the potential liability has been addressed, what can organizations do to mitigate risk and increase compliance?

1. Encrypt the data at rest and in transit—including CD-roms and USB drives.
2. Establish adequate policies and procedures.
3. Monitor telecommuters, and make sure that they have the appropriate firewalls, automatic log-out, and appropriate computer administration.

4. Utilize virtual private networks (VPNs).
5. Make sure that software updates are being implemented.

Conclusion

The transportation of data occurs in a variety of ways—from USB drives to email to the cloud. As Bill Gates indicated, companies cannot look two years down the road. Instead, keeping a pulse on current and proposed regulations, as well as changes in technology options, can enable companies to be better prepared to anticipate and plan for changes. ☉

Endnotes

[1]www.dictionary.reference.com/browse/transport.

[2]45 CFR §160.103 (defining protected health information to include electronic and other forms and mediums that can contain individually identifiable health information, which can be used to identify the individual or creates a reasonable belief that the individual can be identified from the information provided).

[3]45 CFR § 160.103.

[4]Pub. L. 104-191 (1996).

[5]Pub. L. 111-105 (2009).

[6]78 Fed. Reg. 5565 (Jan. 25, 2013).

[7]45 CFR §§ 160.102, 164.500.

[8]78 Fed. Reg. 5565, 5572 (Jan. 25, 2013).

[9]*Id.*

[10]75 Fed. Reg. 40868, 40872-73 (July 14, 2010).

[11]Texas Medical Record Privacy Act (H.B. 300), Section 181(b)(2) (Sept. 1, 2012).

[12]U.S. Department of Justice, Federal Bureau of Investigation (FBI), "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain" (April 8, 2014), *available at* info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

[13]Ponemon Institute, "Fourth Annual Benchmark Study on Patient Privacy and Data Security" (March 2013), *available at* www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security.

[14]SANS, "Healthcare Cyber Threat Report" (Feb. 2014), *available at* pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf.