HIPAA and Mobile Health

Where's the App for That?

by Barry Liss

Benjamin Franklin, the first postmaster general appointed under the Continental Congress, imposed what may have been the nation's first privacy and security rules. Concerned about unauthorized disclosures, loss of privacy, and lax security in the colonial mail system, he ordered local postmasters to segregate their post offices from their homes, only allow authorized individuals to handle the mail, seal mail in a bag, keep the bag sealed until the destination was reached, and require identification of the recipient before allowing someone to receive the posted letter.[1]

Now, the nation has the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH), and other federal and state laws intended to address the same concerns (*i.e.*, unauthorized disclosures, loss of privacy, and lax security). It bears noting that Franklin's privacy and security rules fit the technology of the day (delivery by foot and horseback).

Today, there is a widening gap between privacy and security on one hand and society's voracious appetite for cutting-edge technology on the other. The healthcare delivery system is front and center in this global, socially pervasive phenomenon. The moniker 'mHealth' captures this entire phenomenon in a single word.

What is mHealth?

Mobile health apps run the gamut, from calorie counters and medication reminders to sensor-based vital sign monitoring, wandering monitors for Alzheimer's patients, portable electrocardiogram systems, environmental sensors for asthma patients, fetal heart rate monitoring, and more. Some of these apps are designed for consumer use only and some are linked to information systems located within healthcare facilities and physician offices. They are used as early warning systems and for general patient management. Mobile health apps have been created to relay biomedical information wirelessly to providers (*i.e.*, remote patient monitoring, or RPM), allowing timely, efficient, and effective care management that has been shown to reduce emergency room visits and hospital readmis-

sions. Hospitals that have been penalized by the Centers for Medicare & Medicaid Services (CMS) for readmissions within 30 days of discharge are, not surprisingly, fertile ground for marketing this technology—indeed, they are easy targets.

Biomedical sensors predict falls in Parkinson's patients. Sensors placed on the skin in the form of tattoos sense abnormalities in body chemistries, and sensors placed on ingested pills transfer biological data in real time to the patients and their physicians.

The argument that mHealth can reduce costs by improving medication compliance, reducing hospital admissions, and reducing emergency room utilization is difficult to dispute, and fuels the dramatic growth of this industry.

The global mHealth industry, which by most accounts did not exist when HIPAA was enacted in 1996, was valued as an $85 million business in 2010 and a $33 billion business in 2015. It is projected to grow at an estimated compound annual growth rate of 33 percent per year between 2015 and 2020, and is ultimately poised to become a $59 billion industry by 2020.[2]

Whether, and to what extent, the mHealth juggernaut has outstripped the vision underlying HIPAA's and HITECH's privacy and security requirements is the focus of this article.

HIPAA and mHealth: Harmony or Discord?

HIPAA, HITECH, and the rules promulgated in connection with them, are enforced by the Office of Civil Rights in the U.S. Department of Health and Human Services. The HIPAA Privacy Rule and HIPAA Security Rule establish the fundamental legal parameters for disclosing, storing, and transmitting patient information (*i.e.*, personally identifiable healthcare information, or PHI). It should also be kept in mind that, in addition to HIPAA, HITECH, the Federal Trade Commission Act and other federal and state laws governing certain circumstances may apply (*e.g.*, records relating to substance abuse treatment, HIV status, genetic information, mental health, sexually transmitted diseases, etc.).[3]

Not all patient information is governed by HIPAA. If the transmission or storage of health information does not involve a 'covered entity,' the information is not PHI, and HIPAA does not apply. Therefore, the threshold inquiry regarding HIPAA compliance involves determining whether the entity that possesses the patient information is a covered entity (*i.e.*, whether it is a health plan, healthcare clearinghouse, or healthcare provider that electronically transmits health information in connection with transactions for which HHS has adopted standards, or whether the entity is a 'business associate' (discussed below).[4]

The Privacy Rule

The HIPAA Privacy Rule generally provides that PHI cannot be disclosed by covered entities without a valid patient consent, unless an exception applies. One exception is when the disclosure occurs for "treatment" purposes, defined as: "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."[5]

Thus, disclosures of PHI from a covered entity (*e.g.*, a healthcare provider) to a server upon which a cloud-based mHealth application resides and stores PHI for patient treatment purposes would likely fit within the healthcare treatment exception and, thus, would not require the patient's consent. However, the transmission and storage of that PHI, indeed a permitted disclosure, is governed by a range of regulations.

The Security Rule

Even though the disclosure may be permitted under the HIPAA Privacy Rule, HIPAA also regulates how such information must be kept when at rest and when transmitted. The HIPAA Security Rule establishes legal requirements for securing electronic PHI (ePHI) and imposes highly specific (and burdensome) obligations on covered entities and their business associates to ensure the ePHI is secure.[6] Those sections of the HIPAA Security Rule with which compliance is perhaps most challenging are found in Subpart C of 45 CFR Part 164, and are organized into several general areas: administrative safeguards; physical safeguards; technical safeguards; organizational requirements; and policies and procedures requirements.

The Fundamental HIPAA Compliance Issue

As noted above, the HIPAA Security Rule applies not only to covered entities but to "business associates." Business associates include: "(i)...[a] person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate."[7] This would appear to fit most mHealth vendors. Thus, an mHealth vendor that provides services to a healthcare provider that involves the disclosure of PHI would likely be a business associate. Accordingly, it must enter into a business associate agreement with the healthcare provider, and the mHealth vendor itself must

then comply with the HIPAA Security Rule.[8] More specifically, the mHealth vendor must have the "required" components of the HIPAA Security Rule in place and must also address the rule's "addressable" components (discussed below).

Healthcare providers violate HIPAA if they fail to enter into business associate agreements when required. Such providers could be exposed to legal liability for non-compliance and damages resulting from their disclosure of PHI to the mHealth vendor.[9]

'Required' Components of the Security Rule

So what exactly must the mHealth vendor have in place to comply with the requirements of the business associate agreement? A lot. It must perform a risk analysis on an annual basis and implement "reasonable and appropriate security measures."[10] It must also implement procedures to regularly review system activity, such as audit logs, access reports, and security incidents.[11] And, it must have a sanction policy to address employees who fail to comply with its own policies.[12]

Among other things, business associates must have data backup plans, disaster recovery plans, and emergency operations plans.[13] With respect to physical safeguard requirements, the vendor must have policies and procedures for handling the disposal of ePHI and policies pertaining to the reuse of media upon which ePHI may be or has been stored.[14] Technical safeguards that must be in place include the use of unique user identification and emergency access procedures.[15] The mHealth vendor must also have certain policies and procedures in place to comply with HIPAA's documentation requirements, and the policies must be retained for at least six years, must be made available to responsible persons, and must be periodically updated.[16]

'Addressable' Components of the Security Rule

In addition to the 'required' elements, the HIPAA Security Rule requires that an even greater range of security elements must be 'addressed,' if not strictly followed. That is, the business associate must assess whether the security element (referred to as a "specification") is reasonable and appropriate in the specific environment, in light of the likely contribution to protecting ePHI. Based on that analysis, the business associate must either implement the security element or document why implementation is not reasonable and implement an equivalent alternative measure.[17]

These additional addressable elements form a veritable laundry list of highly specific and technical items, and include such things as:

- Procedures for supervising workforce,[18]
- Procedures to determine if access by certain workforce members is appropriate,[19]
- Procedures for terminating workforce members having access to ePHI,[20]
- Policies for granting access to ePHI,[21]
- Policies and procedures to protect against malicious software, login monitoring, and password management,[22]
- Policies and procedures regarding incident response and reporting,[23]
- Policies and procedures for periodic testing and revision of contingency plans, assessment of criticality of applications and data in support of contingency plan components,[24]
- Procedures to allow facility access in an emergency,[25]
- Policies to prevent unauthorized physical access, tampering and theft,[26]
- Procedures to validate a person's access to facilities based on their function,[27]
- Policies and procedures to document repairs and modification to physical plant relating to security,[28]
- Policies to record the movement of hardware and electronic media and note the person responsible,[29]
- Retrievable exact copy of ePHI when needed before moving equipment,[30]
- Automatic logoff,[31]
- Encryption/decryption processes,[32]
- Mechanisms to authenticate ePHI and corroborate that it has not been improperly altered or destroyed,[33]
- Measures to guard against improper modification of ePHI,[34] and
- Other requirements set forth in Subpart C of 45 CFR Part 164.

What about the Cloud?

Cloud service providers that store PHI for mHealth applications are most likely business associates.[35] As such, they must enter into business associate agreements with either the healthcare provider directly or with the mHealth vendor that engages the cloud service as a subcontractor. Thus, as business associates, they too must meet the required and addressable components of the HIPAA Security Rule.

Enforcement and Practical Risk Mitigation

Exposure to legal liability for non-compliance with HIPAA arises primarily under two circumstances: 1) unauthorized disclosures (*e.g.*, lost or stolen laptops, thumb drives, etc.); and 2) audits conducted by the U.S. Department of Human Services Office of Civil Rights pursuant to the HIPAA Audit Program. The former circumstance, unauthorized disclosure, is a risk that can be mitigated by password-protecting and encrypting all PHI. Additional practical measures include installing remote data-wiping capabilities, installing firewalls, and deleting all PHI before discarding or returning any type of data storage devices.[36]

Encryption, password protection,

and data-wiping capabilities, however, are not substitutes for compliance with the HIPAA Security Rule. Covered entities and business associates would be exposed to legal liability and, potentially, civil monetary penalties imposed by the Office of Civil Rights for failure to comply with the required and addressable components of the rule.[37] This would appear to generally include mHealth vendors and their subcontractors when any of them become business associates.

Is it Time for a HIPAA Reality Check?

While it may be axiomatic that legislation follows technology, the conundrum here is the speed with which the schism between the two is widening. Can the unstoppable mHealth industry co-exist with the regulatory scheme developed before the advent of that very industry? A recent survey of healthcare providers and healthcare systems conducted by Health Information and Management Systems found that 90 percent of respondents use mobile devices to engage patients, yet only 57 percent had a mobile technology policy.[38] These survey results do not prove that the remaining 43 percent are non-compliant with HIPAA, but it begs the question. (On the other hand, neither do the results prove that the policies adopted by 57 percent of the respondents actually comply with HIPAA.)

In its security survey published in January of this year, Arxan Technologies reported that 84 percent of the Food and Drug Administration (FDA)-approved mobile health apps included in the study failed to address at least two of the top 10 risks identified by the Open Web Application Security Project, a worldwide nonprofit organization that focuses on raising awareness about software security.[39] Can these survey results be generalized to all mHealth apps? Do these results suggest potentially broad, large-scale non-compliance with the HIPAA Security Rule?

This issue of HIPAA compliance by mHealth application developers has been brought to the attention of the Office of Civil Rights and, based on her letter of Nov. 2014, Sylvia Burwell, the secretary of the U.S. Department of Human Services, has acknowledged the need to address it.[40] In the meantime, the HIPAA Security Rule is in place and the Office of Civil Rights' HIPAA Audit Program continues.

Conclusion

Providers of healthcare services that transmit patient information electronically are covered entities and, therefore, must comply with the privacy and security rules. Additionally, mHealth vendors that enter into arrangements with healthcare providers, as well as their subcontractors, will typically have to enter into business associate agreements and, thus, must also comply with the HIPAA Security Rule. The rule requires

specific measures be taken by covered entities and business associates. Failure to do so can lead to legal liability. From a practical perspective, encryption of all patient information transmitted electronically and, particularly, encryption of all data residing on moveable electronic media such as laptops, flash drives, and CDs, although not currently required by HIPAA, is urged.

The explosion of mHealth products and services anticipated within the next five years poses a compliance challenge to not only the healthcare providers who use them, but also to the mHealth vendors and developers who market them. ⚖

Barry Liss *is director at Gibbons P.C. His practice is exclusively devoted to healthcare law, representing hospital systems, physician groups, multi-specialty practices, HMOs, health insurance companies, organized delivery systems, and related business enterprises in the healthcare sector.*

ENDNOTES

1. F. Lane, American Privacy: The 400-Year History of our Most Contested Right, Beacon Press (2009), cited in A. M. Helm, and D. Georgatos, Privacy and mHealth: How Mobile Health 'Apps' fit into a Privacy Framework Not Limited to HIPAA, 64 *Syracuse L. Rev*. 131.
2. Kalorama Information, mHealth Markets Worldwide, July 8, 2015, cited in PRNewswire, Kalorama: mHealth Market Expected To Reach $33.7 Billion, July 28, 2015.
3. The Federal Trade Commission monitors and regulates consumer privacy matters, and, accordingly, it also oversees the mHealth industry. It has been argued that mHealth arrangements are more likely to be prosecuted by the FTC than by the Office of Civil Rights. *See* A. M. Helm, and D. Georgatos, cited above, 64 *Syracuse L. Rev*. 131.
4. 45 CFR 160.102.
5. 45 CFR 164.501.
6. 45 CFR 164.104.
7. 45 CFR 160.103.
8. 45 CFR 164.104(b).
9. 45 CFR 308(b)(3); 45 CFR 164.314(a).
10. 45 CFR 164.308(a)(1)(ii)(A).
11. 45 CFR 164.308(a)(1)(ii)(D).
12. 45 CFR 164.308(a)(1)(ii)(C).
13. 45 CFR 164.308(a)(7)(ii).
14. 45 CFR 164.310(d)(2).
15. 45 CFR 164.312(a)(2).
16. 45 CFR 164.316(b)(2).
17. 45 CFR 164.306(d)(3).
18. 45 CFR 164.308(a)(3)(ii)(A).
19. 45 CFR 164.308(a)(3)(ii)(B).
20. 45 CFR 164.308(a)(3)(ii)(C).
21. 45 CFR 164.308(a)(4)(ii)(B).
22. 45 CFR 164.308(a)(5)(ii)(B).
23. 45 CFR 164.308(a)(6)(ii).
24. 45 CFR 164.308(a)(7)(ii)(E).
25. 45 CFR 164.310(a)(2)(i).
26. 45 CFR 164.310(a)(2)(ii).
27. 45 CFR 164.310(a)(2)(iii).
28. 45 CFR 164.310(a)(2)(iv).
29. 45 CFR 164.310(d)(2)(iii).
30. 45 CFR 164.310(d)(2)(iv).
31. 45 CFR 164.312(a)(2)(iii).
32. 45 CFR 164.312(a)(2)(iv).
33. 45 CFR 164.312(c)(2).
34. 45 CFR 164.312(e)(2)(i).
35. 78 FR 5572.
36. *Take Steps to Protect and Secure Information When Using a Mobile Device*, published by HealthIT.gov.
37. Subpart D of 45 CFR Part 160.
38. 2015 HIMSS Mobile Technology Study Executive Summary, April 2015.
39. Failures most often included lack of binary protections and insufficient transport layer protection. 5th Annual State of Application Security Report, Perception vs. Reality, Health Care Edition, Arxan Technologies, Jan. 2016.
40. Letter from Sylvia Burwell, Secretary of U. S. DHSS to Hon. Tom Marino, Nov. 21, 2014.