Tips and Tactics for Transmitting PHI by Email

By Angela T. Burnette and Swathi Padmanabhan, Alston & Bird LLP, Atlanta, GA

Email is not like mailing a sealed letter or package. It is more like sending a postcard—people are not supposed to read it while in transit, but it passes through many hands, and one can never be sure that someone is not reading it illegally.[1]

In 2013, approximately 100 billion business emails were sent and received on a daily basis.[2] At the intersection of convenience and speed, special considerations come into play when an email contains or attaches identifiable health information. HIPAA Covered Entities and Business Associates should assess under what criteria and safeguards such information is being transmitted via email in their particular environments. While the HIPAA Security Rule provides some flexibility in tailoring individual security practices, this article outlines additional considerations, including lessons learned from previous email breaches reported to the Department of Health and Human Services (HHS).

Overview

Under the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HHS issued regulations to address the privacy and security of health information (the Privacy and Security Rules)

and to facilitate electronic submission of health care transactions. This article focuses on the use of email to transmit Protected Health Information (PHI) for reasons other than electronically submitting health care transactions.

Found at 45 C.F.R. Parts 160 and 164, the HIPAA Privacy and Security Rules apply to Covered Entities, and certain portions of these Rules apply to Business Associates. Generally, Covered Entities are health plans, health care providers who engage in certain health care transactions electronically, and health care clearinghouses. Business Associates are persons or entities that provide services to or for a Covered Entity and, as part of providing those services, receive or have access to PHI from or on behalf of such Covered Entity. Examples of Business Associates include accountants, auditors, and lawyers.

While the Security Rule protects Electronic PHI,[3] consider general Privacy Rule requirements with respect to all PHI transmitted by email. For example, an email's wording could contain PHI or a medical record could be scanned into a PDF and attached to an email. A fax could be delivered as a PDF to an email address or a voicemail could be converted to an audio file and delivered via email. Even if emails are deleted from the primary system, many email systems use cached storage on mobile devices so the data may still reside there. While email can be efficient, private, and secure, consider whether additional options might be appropriate and practical for your particular work environment.

Is There Another, Equally Effective Way to Send the PHI?

While email use is prevalent, email need not be the default method of communication, especially when other methods would be as practical or even preferable. For example, an alternative to email may be desirable if the PHI being disclosed is sensitive information specifically protected by state law, e.g., HIV, AIDS, genetics, mental health, substance abuse, venereal diseases, or privileged communications. Additionally, an alternate method may be appropriate if the intended recipient cannot support the encryption or secure email messaging method the sender would use to transmit the PHI.

In some situations, a simple telephone call to the recipient might suffice instead of an email. An alternative also could involve establishing a secure extranet with encryption and limited access rights, particularly if several PHI files are involved and ongoing access is desired. If an extranet is not practical, storage media such as a CD, DVD, or flash drive could be delivered by overnight courier; encryption could be used so that if the media is lost or misdelivered, the unintended recipient cannot access or retrieve the PHI. The key to decrypt the PHI should not be stored on the same device containing the encrypted data. Instead, the key could be separately communicated to the intended recipient and generated after the intended recipient enters a protected password. (As discussed below, encryption methods should comply with National Institute of Standards and Technology (NIST) standards to take advantage of the breach reporting safe harbor provided by the Health Information Technology for Economic and Clinical Health (HITECH) Act.)

Is Disclosing the PHI Necessary?

Many uses and disclosures of PHI are governed by HIPAA's minimum necessary standard. Generally, this means the PHI sought and disclosed should be limited only to that information reasonably necessary to accomplish the purpose of the disclosure.[4] Even when one of the exceptions to HIPAA's minimum necessary standard applies, the principle can provide helpful guidance in protecting the privacy and confidentiality of PHI.

When sending PHI by email, consider whether it is necessary for the email to disclose PHI and, if so, whether the email must disclose the extent of the PHI being transmitted. If a medical record sent to a law firm was received by the wrong lawyer, an email could be sent to other lawyers and paralegals within the firm inquiring as to the intended recipient without disclosing the patient's name, diagnosis or other PHI. For example, such an email could state, "I just received a medical record from XYZ hospital for a female patient. If you believe this record should have been delivered to you, please give me a call." The essential purpose of the message was communicated without including the patient's name, date of birth, or other PHI. If an email must refer to a patient for identification purposes, consider whether the patient's first and last initials could be used rather than the patient's full name. Also, before emailing particularly sensitive information, such as a patient's date of birth, driver's license number, Social Security number, or state-law protected diagnosis, consider whether such details are necessary to accomplish the email's purpose.

Even if the PHI is the minimum amount necessary, think through which persons within your workforce have access to such PHI and whether they need such access to perform their duties. For example, consider who has access rights to the email accounts of the sender and/or recipient. If access is needed, what are the conditions or criteria appropriate to that access? Consider whether emails that contain or attach PHI can be moved to or stored in a particular folder, drive, or other location that has limited access rights, such as only the particular project team and IT personnel.

Is the Disclosure of PHI by Email Affected by Your Other Obligations?

Contracts, including business associate agreements, should be considered regarding whether they contain broad limitations that might affect disclosure of PHI via email. For example, a contract might expressly prohibit providing access to or sending PHI to contractors offshore, e.g., outside the United States and U.S. territories. Additionally, a services contract, engagement letter, or provider agreement might contain comprehensive language regarding how information will be used, disclosed, transmitted, or stored.

Covered Entities also have a duty to abide by their Notice of Privacy Practices (NPP).[5] Because a NPP typically describes the various purposes for which PHI can be used/disclosed, it is unlikely that a NPP specifically addresses the use of email. However, it is worth reviewing the NPP to see if email is captured in some broad concept and/or considering whether to add a statement to the NPP regarding use of email generally.

A Covered Entity or Business Associate should comply with its applicable Terms of Use, Privacy Policy, and other representations made to consumers. For example, if a Privacy Policy on a website states that PHI will not be transmitted by email absent an individual's prior written consent, then such consent should be obtained or the Privacy Policy should be revised accordingly.

Under HIPAA, an individual has the right to request restrictions and request confidential communications.[6] If a Covered Entity agrees to an individual's request involving email, the agreed upon restriction should be communicated to persons within the Covered Entity's workforce (and to any Business Associate) who would need that information to perform their job duties. Additionally, if the individual exercises his right to restrict disclosure of PHI to a health plan regarding an item or service already paid for in full, such PHI should not be inadvertently included in an email sending batches of several patients' files to the health plan for quality assurance purposes.

Whether to Encrypt and, If So, What Type of Encryption?

The HIPAA Privacy and Security Rules do not necessarily require the use of encryption. Whether to encrypt is an addressable specification under the HIPAA Security Rule, and the following factors can be used by a Covered Entity or Business Associate in deciding what security measures to use: (1) its size, complexity, and capabilities; (2) its technical infrastructure, hardware, and software security capabilities; (3) the costs of security measures; and (4) the probability and criticality of potential risks to Electronic PHI.[7] In issuing the 2003 Final Security Rule, HHS commented that when Electronic PHI "is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk."[8] Where a risk analysis shows Electronic PHI being transmitted "would be at significant risk of being accessed by unauthorized entities," HHS "would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption."[9]

There may be several encryption programs advertised in the marketplace. As encryption options are considered, assess whether encryption that is advertised as "HIPAA compliant" actually meets NIST standards for encryption, both for data at rest and data in motion. Also, consider encryption options for remote sessions that could access PHI from another location or through the Internet. The benefits of NIST-compliant encryption are significant. In the event of an incident involving an impermissible disclosure of, or access to, PHI in violation of HIPAA, NIST-compliant encryption provides a safe harbor from reporting obligations that might otherwise apply. Generally, if Electronic PHI is encrypted to NIST standards, it is considered by HHS to be sufficiently secure that such PHI would not be considered "Unsecured PHI" and such an incident would not be a reportable breach.

When communicating with individuals who are the subject of the PHI being sent, unencrypted emails are permitted, but HHS expects a Covered Entity to "notify the individual that there may be some level of risk that the information in the email could be read by a third party."[10] If individuals are "notified of the risks and still prefer unencrypted email," they have the right to receive the unencrypted PHI per their request, and Covered Entities are not responsible for unauthorized access of PHI during such transmissions.[11]

Disposal of Emails Containing PHI

When emails are no longer needed, they should be disposed of in a manner consistent with published HHS guidance.[12] As HHS has emphasized, "Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI."[13]

Covered Entities and Business Associates should consider developing and implementing PHI disposal policies/procedures and providing such training to workforce members. Factors to consider when developing these policies include: (a) the potential risks for patients; (b) whether the PHI to be disposed is in electronic or hard copy form; (c) the type and amount of PHI to be disposed; and (d) whether the PHI to be disposed consists of names, Social Security numbers, driver's license numbers, financial information, or other sensitive information whose inappropriate disclosure could expose patients to identity theft, discrimination, or reputational harm.[14]

Printouts of emails containing PHI should not be placed in dumpsters, garbage cans, or other trash receptacles accessible to the public. Proper disposal could include "shredding or otherwise destroying PHI in paper records so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed prior to it being placed in a dumpster or other trash receptacle."[15] Consider maintaining the email printouts in a secure area (or in a locked dumpster) until a third-party vendor, such as a Business Associate, shreds or otherwise disposes of such emails in a manner that renders them unreadable. Consider, also, efforts to minimize or discourage workforce members from recycling emails that contain PHI.

CDs, DVDs, thumb drives, and other electronic media should be stripped of Electronic PHI before being recycled or reused. Keep in mind, also, that email might be stored in other systems outside of the messaging system, such as archiving repositories and document management systems. Depending on the circumstances, appropriate methods may include clearing (sensitive information is written over and replaced with non-sensitive data), purging (exposing the media to a strong magnetic field), or destroying the media (electronic media is disintegrated, pulverized, melted, shredded, or incinerated).[16]

Email Breach Incidents Reported to HHS

Approximately 40 breaches involving email have been reported thus far to HHS as affecting more than 500 individuals.[17] What potential lessons can be gleaned from such incidents?

Blind carbon copy recipients, rather than listing them on the "To" line, when communicating with multiple individuals. A Maryland hospital reported in 2010 that a business associate sent an email to multiple patients participating in a dietary program; the email disclosed patient names and email addresses to all other recipients. In total, 937 individuals were affected.[18]

Check recipients' email addresses and attachments before sending, particularly before sending numerous files to numerous recipients. A private practice in New York inadvertently attached confidential information of about 10,200 current/former patients to an email it sent to 200 patients. The attachment reportedly included patient names, home addresses, dates of last appointment, scheduling codes, primary physicians, referring physicians, and email addresses.[19] In another reported breach, a benefits staff member at a hospital affiliated health plan emailed 85 employees and inadvertently attached PHI of almost 700 employees' dependents.[20]

Confirm a proper basis and method for sending PHI to a third-party recipient before sending. A children's hospital in Ohio reported a 2010 breach involving an unencrypted list of patient names and addresses that was emailed from the hospital to a local nonprofit agency for use in inviting those patients to attend a summer camp.[21] The information involved 1,000 individuals but did not include Social Security numbers, telephone numbers, specific medical information, or credit card/financial information.

Consider encryption or a secure email messaging system if one is available; otherwise, consider a different means of communication. A Texas hospice reported a breach affecting 800 patients after an employee sent two unsecured emails containing patient names, referral sources, admission and discharge dates, names of insurance providers, and chart numbers.[22] In another reported incident, a hospital employee in Tennessee sent three emails that transmitted PHI of over 1,000 patients in an unsecure manner.[23] The unsecure emails contained patient names, dates of birth, account numbers, telephone numbers, and Social Security numbers.

Avoid sending PHI to a personal email account. In 2010, a physician at a hospital in Pennsylvania emailed unencrypted PHI to his personal email account to finish analyzing certain procedures. After the hospital notified him of the incident, the physician then contacted his home email provider and gave permission for the PHI to be deleted from that provider's network and servers. The physician also deleted the PHI from his home computer. The incident involved approximately 3,000 patients' names, medical record numbers, procedure indications, and physician notes.[24] Similarly, in another reported breach, an employee of a state agency inappropriately emailed to his personal account 17 spreadsheets containing nearly 230,000 patients' Social Security numbers, telephone numbers, mailing addresses, birth dates, and Medicaid ID numbers.[25]

At the intersection of convenience and speed, special considerations come into play when an email contains or attaches identifiable health information.

Follow established encryption procedures; if encryption is not available or is not supported by the recipient, consider alternate means of communicating the PHI. In the Pennsylvania hospital breach reported above, the physician failed to follow established procedures when he chose to send unencrypted PHI to his personal email account. If an employee believes further work from home is necessary, an alternative might include using a secure/encrypted flash drive or connecting from home to the employer's network through a secure means of remote access.

Educate your workforce about phishing emails and that such emails should be reported to IT personnel for follow up. In 2012, a Kentucky state agency employee reportedly responded to a phishing email sent by a hacker.[26] Fortunately, improper activity on the email account was quickly identified and the account was disabled. The agency notified approximately 2,500 individuals because the hacker reportedly had access to the employee's email account for a brief period of time. The account included access to individual names, birth dates, and addresses. In another incident reported in late 2013, an employee at a nonprofit organization was deceived by an email phishing scam.[27] While investigating the incident, the organization learned that other employees also had been tricked by phishing activity.[28] Almost 4,000 individuals were reportedly affected, and the information possibly included driver's license numbers, birth certificates, Medicaid/Medicare numbers, Social Security numbers, and financial information.[29]

Consider the extent of PHI that is necessary. Consider whether it is feasible to avoid sending patients' telephone numbers, driver's license numbers, Social Security numbers, birth dates, credit/debit card information, or insurance/financial informa-

While email use is prevalent, email need not be the default method of communication, especially when other methods would be as practical or even preferable.

tion by email unless encryption or another secure method is used. In some of the breaches described above, such information was not involved, which may have helped to reduce potential damage and maintain customer/public confidence.

Additional Tips for Consideration

- Consider the criticality of the recipient's request for PHI, whether encryption or secure messaging is being used and/or whether another communication method is advisable.
- Be aware of the risk that an email address could be incorrectly typed or auto-filled.
- Avoid disclosing an individual's PHI in the subject line of an email; encryption methods might not encrypt the subject line.
- Avoid auto-forwards of email accounts, especially to external destinations.
- Instead of forwarding an email that contains an attachment of PHI, consider creating and encrypting a PDF to be sent; the password key for decryption should not be sent in the same email transmitting the PDF.
- Avoid emailing PHI to/from a personal email account/home computer; consider accessing PHI instead through secure remote access or via encrypted/otherwise secure portable devices. (An attachment sent to a personal email account and then opened could still leave some sort of file on the machine from which it was accessed.)
- Limit patient identifiers where practicable, especially where the information is specifically protected by state law or could be used to perpetrate identity theft.
- When communicating with a patient, use the email address specifically provided by the patient for that purpose. The patient may have provided a work email address rather than a home email address for a specific reason. Also, consider notifying patients of the risks involved in email, particularly unencrypted email, and confirm that patients still desire email communications. For example, patients could acknowledge that not all email is necessarily confidential and that another method should be used to communicate sensitive information. Finally, be cautious about responding to emails that request that you send PHI; the listed sender of the email may or may not be the actual author.
- Change passwords to email accounts regularly and do not keep passwords written down near or on the computer/device.
- Consider including a notice of confidentiality in emails that instructs recipients on the steps to take if they are not the intended recipients, such as notifying the sender and deleting the email and all copies.
- Develop a written policy regarding email and train your workforce, including on whom to contact if a security incident or breach occurs.

Conclusion

While email is common and convenient, privacy considerations are involved in emailing PHI. Keeping in mind HIPAA obligations, lessons learned from other breaches, and the practical tips outlined above may help to limit the amount of Electronic PHI transmitted by email. If a theft, loss, or other breach incident occurs, the less Electronic PHI involved in an email the better, especially if the PHI involves sensitive information, is unencrypted, or involves numerous individuals. C

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm or its clients. This article is for general information purposes only. It is not intended to be and should not be relied upon as legal advice.

About the Authors

Angela T. Burnette (angie.burnette@alston.com) is Counsel in Alston & Bird's Health Care Group, and she practices in Alston & Bird's Atlanta office. She provides general risk management and compliance advice to health care facilities, providers, and health plans. She also advises clients on HIPAA privacy, HIPAA security, and breach notification issues under the HITECH Act and state laws. In addition, Ms. Burnette handles health care litigation involving issues such as hospital-physician disputes, hospital licensure and peer review, successfully resolving matters at the trial and the appellate level. She also represents health care providers in state licensing board investigations. While at Alston & Bird, Ms. Burnette has served as both temporary in-house counsel and as national coordinating counsel for two national health care corporations.

Swathi Padmanabhan (swathi.padmanabhan@alston.com) is an associate in Alston & Bird's Health Care Group, practicing in the firm's Atlanta office. She focuses her practice on corporate and regulatory health care matters. Her experience includes assisting clients with mergers and acquisitions and securities law matters as well as with HIPAA privacy, HIPAA security, and breach notification compliance. Ms. Padmanabhan received her J.D. from Vanderbilt University Law School and her A.B. in public policy from Duke University.

Endnotes

1 *HIPAA Security Rule: Frequently Asked Questions Regarding Encryption of Personal Health Information*, Am. Med. Ass'n (2013), *available at* www.ama-assn.org/resources/doc/washington/hipaa-phi-encryption.pdf.
2 Sara Radicati, Ph.D., Justin Levenstein, *Email Statistics Report*, 2013-2017 Executive Summary, The Radicati Group, Inc., (Apr. 2013), *available at* www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf.
3 *See* 45 C.F.R. § 160.103 (definition of electronic protected health information).
4 *See* 45 C.F.R. §§ 164.502(b) and 164.514(d).
5 *See* 45 C.F.R. § 164.520(b)(1)(v)(B).
6 45 C.F.R. § 164.522(a)-(b).
7 45 C.F.R. § 164.306(b)(2).
8 Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8334, 8356 (Feb. 20, 2003) (HIPAA Final Security Rule).
9 *Id.* at 8357.
10 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5566, 5634 (Jan. 25, 2013).
11 *Id.*
12 *See Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, available at* www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html (last visited Jan. 8, 2014).
13 *Frequently Asked Questions About the Disposal of Protected Health Information,* Dep't of Health & Human Servs., *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf; *see also Disposal of Protected Health Information,* Dep't of Health & Human Servs., *available at* www.hhs.gov/ocr/privacy/hipaa/faq/disposal_of_protected_health_information/ [hereinafter, collectively, Disposal of PHI].
14 Disposal of PHI, *supra* note 13.
15 *Id.*
16 *See id.*
17 *Breaches Affecting 500 or More Individuals,* Dep't of Health & Human Servs., *available at* www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Jan. 13, 2014) [hereinafter Breaches].
18 *Id.*
19 Mass Email Inadvertently Breaches Privacy of 10,200 Patients, PHIprivacy.net (May 15, 2013, 6:47 AM), *available at* www.phiprivacy.net/mass-email-by-dent-neurologic-inadvertently-breaches-privacy-of-10200-patients/.
20 Breaches, *supra* note 17.
21 *Public Notice Of Security Breach At Dayton Children's*, WHIOTV (June 18, 2010, 11:19 AM), *available at* www.whio.com/news/news/public-notice-of-security-breach-at-dayton-childre/nHnMg/.
22 Patrick Ouellette, *Hope Hospice Informs 800 Patients of Health Data Breach*, HealthITSecurity (Apr. 29, 2013), *available at* http://healthitsecurity.com/2013/04/29/hope-hospice-informs-800-patients-of-health-data-breach/.
23 Erin McCann, *Email Gaffe Begets Memphis Data Breach*, Healthcare IT News (May 13, 2013), *available at* www.healthcareitnews.com/news/email-gaffe-begets-memphis-data-breach.
24 Paul Barr, *Geisinger Announces Data Breach, Modern Healthcare* (Dec. 28, 2010), *available at* www.modernhealthcare.com/article/20101228/NEWS/312289995.
25 Zoheb Hassanali, *Thousands of Confidential Medicaid Records Stolen, Wachfox* (Apr. 19, 2012, 10:13 AM), *available at* www.wach.com/news/story.aspx?id=743902#.UsAtZWRDuPT (last updated Apr. 19, 2012, 1:15 PM).
26 Joseph Conn, *Ky. Health Agency Discloses Possible Data Breach,* Modern Healthcare (Sept. 19, 2012), *available at* www.modernhealthcare.com/article/20120919/NEWS/309199955.
27 *More on Today's HHS Update: Newly Disclosed Incidents*, PhiPrivacy.net, *available at* www.phiprivacy.net/more-on-todays-hhs-update-newly-disclosed-incidents/ (Jan. 10, 2014).
28 *Id.*
29 *Id.*