PRACTICE RESOURCE

Health Care Data Breaches: Practical Advice for Trying Times

Kristen Rosati and Scott Bennett

What is the issue? Health care organizations and their business associates are increasingly vulnerable to data breaches. The causes of breaches range from simple human error to intentional theft and hacking incidents.

What is at stake? Dealing with a data breach is expensive, especially for health care organizations because of the extensive breach-reporting requirements of the Health Insurance Portability and Accountability Act and state breach laws. Breaches can also lead to extensive (and expensive) government investigations, fines, civil lawsuits, and the loss of customers and business reputation.

What should attorneys do? Having a good security risk management program and incident response plan in place will reduce the potential costs of a breach. In this Practice Resource, the authors provide practical suggestions for effective breach planning and response.

CITATION: Kristen Rosati and Scott Bennett, *Health Care Data Breaches: Practical Advice for Trying Times*, J. Health & Life Sci. L., Feb. 2017, at 90,

Author biographies appear on the next page.

Kristen Rosati is a Partner at Coppersmith Brockelman. She is considered one of the nation's leading HIPAA compliance attorneys and has deep expertise with large data breaches, health information exchange, data sharing for research and clinical integration initiatives, electronic health record roll-outs, clinical research compliance and contracting, biobanking, and all matters related to "Big Data." Contact her via email at krosati@cblawyers.com.

Scott Bennett is a Partner at Coppersmith Brockelman, where his practice focuses on representing hospitals and other health care providers. He has helped many health care clients respond to—and mitigate the potential harm from—data breaches. He also has significant experience conducting internal investigations and representing clients in government investigations, criminal and civil litigation, and administrative proceedings. Contact him via email at sbennett@cblawyers.com.

Rosati and Bennett: Data Breaches

CONTENTS

Introduction

According to a study released in May 2016, nearly 90% of health care organizations surveyed had experienced a data breach in the past two years, and 45% had dealt with more than five breaches in the same time period.[1] The average estimated cost of a breach for a health care organization is $2.2 million.[2] For a business associate, the estimated cost is more than $1 million.[3] Breaches cost the health care industry an estimated $6.2 billion every year.[4]

The costs of a breach are higher in health care than in other industries, presumably because of the breach-reporting requirements of the Health Insurance Portability and Accountability Act (HIPAA). A study released in June 2016 found that the average cost of a data breach in the United States was $221 per compromised record; but for health care breaches, it was $355 per record.[5]

The number of patients affected by health care breaches is staggering. In 2015, the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS), the federal agency responsible for enforcing HIPAA, was notified of 253 breaches that collectively involved more than 112 million records.[6]

A data breach represents a significant problem that all organizations must be prepared to handle. The potential consequences include

---

1 Ponemon Inst., Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 1 (2016), *available at* www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm_source=Referral&utm_medium=press%20release&utm_campaign=Ponemon%202016 [hereinafter Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data].

2 *Id*.

3 *Id*.

4 *Id*.

5 Ponemon Inst., 2016 Cost of Data Breach Study: Global Analysis 5, 10 (2016), *available at* www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN [hereinafter 2016 Cost of Data Breach Study].

6 Dan Munro, *Data Breaches in Healthcare Totaled Over 112 Million Records In 2015*, Forbes (Dec. 31, 2015, 9:11 PM), www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#731780157fd5.

government investigations and fines, lawsuits by affected individuals, financial harm, customer loss, and reputational injury. Research suggests, however, that by taking steps to prevent and prepare for a breach, organizations can meaningfully reduce those costs.[7]

This Practice Resource will explain HIPAA's breach-reporting requirements, as well as address the requirements of state breach laws. The Practice Resource then provides specific suggestions that companies can follow to prepare for and respond to breaches.

The authors conclude that the health care industry regulators should examine whether breach-reporting requirements should be changed. Health care companies already are operating on a thin profit margin, and the substantial expense of reporting may force some of those companies out of business. More practical alternatives might protect individuals by requiring individual authentication for obtaining credit and other services, and instituting smarter payment algorithms to catch fraudulent claims. Ultimately, what would help consumers most is a system that requires reporting in those situations where individuals need to know about the breach to protect themselves.

HIPAA's Breach Reporting Requirements

The terms "security incident" and "breach" have specific definitions under HIPAA. Although a security incident generally means "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices,"[8] the HIPAA definition is more specific: "Security incident means the attempted or successful unauthor-

7 Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, at 2.

8 Nat'l Inst. of Standards & Tech., Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology 6 (2012), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. *See also* Rick Kam, *What's in a Name? Defining Event vs. Security Incident vs. Data Breach*, ID Experts Blog, Jul. 8, 2015, www2.idexpertscorp.com/blog/single/whats-in-a-name-defining-event-vs.-security-incident-vs.-data-breach.

ized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[9]

Under HIPAA's Breach Notification Rule, a breach is defined as the unauthorized "acquisition, access, use, or disclosure of protected health information [PHI] in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI]."[10] Examples of breaches include the loss of an unencrypted thumb drive that contains PHI, a hospital employee snooping through the medical records of a celebrity patient, a doctor's office disposing of paper records that contain PHI in a publicly accessible dumpster, or hackers accessing PHI in a hospital's computer system.

Determining whether an incident is a reportable breach under HIPAA requires answering four questions: (i) Was there unauthorized acquisition of, access to, or use or disclosure of PHI? (ii) Was the PHI unsecured? (iii) Does an exception to the definition of breach apply? (iv) Can the covered entity or business associate demonstrate a "low probability that the PHI has been compromised?"[11]

First, it is important to note that a violation of the Security Rule does not, by itself, create a reporting obligation unless the violation causes an unauthorized use or disclosure of PHI. As just one example, the Security Rule requires covered entities and business associates to perform a periodic evaluation to determine whether their policies and procedures meet the requirements of the Rule.[12] A failure to conduct that evaluation would not, by itself, constitute a reportable breach.

Second, HIPAA requires notifications for breaches of "unsecured" PHI.[13] PHI is secure if it has been "rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of Health and Human

9 45 C.F.R. § 164.304.
10 45 C.F.R. § 164.402.
11 *Id.*
12 *Id.* § 164.308(a)(8).
13 *Id.* §§ 164.404(a)(1), .406(a), .408(a), .410(a)(1).

Services (HHS)]. . . ."[14] PHI is considered secure for purposes of the Breach Notification Rule if it has been encrypted according to standards issued by the National Institute of Standards and Technology, or if the media on which the PHI was stored has been destroyed as specified.[15] If the PHI was secured accordingly, no reporting is required. If, however, PHI was unsecured, the entity must proceed to the third question.

Although encryption of devices and data helps to avoid a reportable breach, the OCR has noted the limits of full or whole disk encryption. Full disk encryption "encrypts the entire disk including swap files, system files, and hibernation files. If an encrypted disk is lost, stolen, or placed into another computer, the encrypted state of the drive remains unchanged, and only an authorized user can access its contents."[16] In July 2016 guidance regarding ransomware, the OCR cautioned that full disk encryption makes the data on a hard drive secure only when the system is powered down.[17] "Once the computer system is powered on and the operating system is loaded, . . . many full disk encryption solutions will transparently decrypt and encrypt files accessed by the user."[18]

This means if a laptop with full disk encryption is powered off, and is then lost or stolen, the data on the hard drive would be considered secure PHI, so the incident would not be a reportable breach under HIPAA.[19] In contrast, if the laptop "is powered on and in use by an authenticated user," and the laptop is lost, stolen, or attacked by ransomware, any PHI on the laptop would not be secure, so reporting might be

---

14 *Id*. § 164.402 (defining *unsecured* PHI).
15 OCR, *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, HHS.GOV, www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html (last visited Nov. 20, 2016).
16 SYMANTEC, WHITE PAPER: HOW WHOLE DISK ENCRYPTION WORKS 1 (2010), *available at* www.symantec.com/content/en/us/enterprise/white_papers/b-pgp_how_wholedisk_encryption_works_WP_21158817.en-us.pdf [hereinafter WHITE PAPER: HOW WHOLE DISK ENCRYPTION WORKS].
17 OCR, FACT SHEET: RANSOMWARE AND HIPAA 8, *available at* www.hhs.gov/sites/default/iles/RansomwareFactSheet.pdf [hereinafter FACT SHEET: RANSOMWARE AND HIPAA].
18 *Id*.
19 *Id*.

required.[20] In that situation, the data on the laptop would be considered secure only if the individual files were encrypted.[21]

Third, HIPAA's Breach Notification Rule excludes three situations from the definition of breach:

1. The unintentional acquisition, access, or use of PHI by a workforce member.
2. An inadvertent disclosure of PHI by an authorized person to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement.
3. Disclosures of PHI where the entity has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

If one of the three exceptions applies, the covered entity or business associate should document that determination, and notification is not required.[22]

Finally, if no exception applies, unauthorized acquisition of, access to, or use or disclosure of unsecured PHI is presumed to be a breach unless the covered entity or business associate "demonstrates that there is a low probability that the protected health information has been compromised . . . ."[23] The covered entity or business associate must assess all relevant factors, including at a minimum the following four factors:[24]

1. **The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification:** Could the information, such as social security number or birth date, be

20 *Id.*
21 White Paper: How Whole Disk Encryption Works, at 1 (explaining the difference between whole disk and file encryption).
22 45 C.F.R. § 164.402(1).
23 *Id.* § 164.402(2).
24 *Id.* § 164.402(2)(i)–(iv).

used in a way that harms the individual (e.g., to commit identify theft)?

2. **The unauthorized person who used the PHI or to whom the disclosure was made:** For example, if the PHI was impermissibly disclosed to another HIPAA-obligated entity, there might be a lower probability that the PHI has been compromised.[25]
3. **Whether the PHI was actually acquired or viewed:** For example, if a forensic analysis shows that the PHI on a lost and recovered computer was never accessed or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual, even though the opportunity existed.[26] (Note that the OCR has stated that an entity may not unduly delay reporting to conduct forensic analysis on a recovered laptop.[27])
4. **The extent to which the risk to the PHI has been mitigated:** For example, the covered entity or business associate could obtain the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means), or that it will be returned or destroyed.[28]

In July 2016, the OCR issued guidance stating that this same four-factor risk assessment is required for ransomware attacks, which are an increasing threat for health care organizations.[29] The OCR stated:

---

25 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, 78 Fed. Reg. 5566, 5643 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).
26 *Id*.
27 *Id*. at 5646.
28 *Id*. at 5643.
29 Jocelyn Samuels, *Your Money or Your PHI: New Guidance on Ransomware*, HHS.GOV, July 11, 2016, www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html; FACT SHEET: RANSOMWARE AND HIPAA; *see also* Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED, Mar. 30, 2016, www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

"When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."[30] The OCR will presume that a ransomware incident is a reportable breach "[u]nless the covered entity or business associate can demonstrate that there is a '. . . low probability that the PHI has been compromised,' based on the factors set forth in the Breach Notification Rule . . . ."[31]

Covered entities and business associates bear the burden of proof when it comes to demonstrating that an incident results in a low probability of compromise.[32] If the entity concludes there is a low probability, it should document its reasons. A covered entity or business associate may also opt to provide notice without conducting a risk assessment.[33]

Covered entities: providing notice to individuals, the OCR, and media

A HIPAA-covered entity must provide notice to "each individual whose unsecured protected health information has been, or is reasonably believed . . . to have been, accessed, acquired, used, or disclosed as a result of such breach."[34] The notice must be in writing and sent by first-class mail, or by e-mail if the affected individual has agreed to electronic notice.[35]

If the covered entity has insufficient contact information for fewer than 10 individuals, the entity may provide substitute notice by alternative written notice, telephone, or other means.[36] If the covered entity has insufficient contact information for 10 or more individuals, the entity must

30 Fact Sheet: Ransomware and HIPAA. at 5–6.
31 *Id*. at 6.
32 45 C.F.R. § 164.414(b).
33 78 Fed. Reg. at 5643.
34 45 C.F.R. § 164.404(a)(1).
35 *Id*. § 164.404(d).
36 *Id*. § 164.404(d)(2)(i)-(ii).

provide substitute notice by either posting the notification on the home page of its website (for at least 90 days) or by providing the notice in major print or broadcast media where the affected individuals likely reside.[37] The covered entity must also include a toll-free phone number that individuals can access for at least 90 days to learn more about the incident.[38]

Based on the authors' experience, in nearly every significant breach, the entity will lack accurate contact information for 10 or more people. Entities should therefore assume they need to provide substitute notice, unless proven otherwise.

Individual notification must be provided to affected individuals without unreasonable delay, and no later than 60 days following discovery of the breach.[39] A breach is "discovered" as of the first day on which the incident is known or should reasonably have been known to the covered entity.[40] (Some states' laws might require a shorter reporting period, as discussed later.)

A covered entity also must notify the OCR of every breach of unsecured PHI via an online form.[41] If a breach affects 500 or more individuals, covered entities must notify the OCR at the same time that they notify affected individuals.[42] Breaches of 500 or more are posted on the OCR's website,[43] known in the industry as the "Wall of Shame." If a breach affects fewer than 500 individuals, the covered entity may notify the OCR of all such breaches annually.[44]

Finally, if a covered entity experiences a breach that affects more than 500 residents of a particular state or jurisdiction, the entity must provide

37 *Id.* § 164.404(d)(2)(ii).
38 *Id.* § 164.404(d)(2)(ii).
39 *Id.* § 164.404(a)(1) & (b).
40 *Id.* § 164.404(a)(2).
41 *Id.* § 164.408; OCR, *Breach Reporting*, HHS.GOV, www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/ (last visited Nov. 20, 2016).
42 45 C.F.R. § 164.408(a).
43 OCR, *Breaches Affecting 500 or More Individuals*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 20, 2016).
44 45 C.F.R. § 164.408(b).

notice to "prominent media outlets" serving that state or jurisdiction.[45] The OCR has explained, however, that breaches involving residents of multiple states might not require media notice. For example, if a covered entity discovers a breach of 700 individuals, 300 from Illinois, 300 from Wisconsin, and 100 from Ohio, the breach would not affect more than 500 residents of any one state or jurisdiction, and therefore media notice would not be required.[46] Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, a prominent media outlet may be a major general interest newspaper that circulates daily throughout the city, rather than the entire state.[47]

Entities could consider providing media notice in a manner that also meets the requirements of substitute notice, which are slightly different. Like individual notice, notice to the media must be provided without unreasonable delay, and in no case later than 60 days following the discovery of a breach. The notice must include the same content required for notification to individuals.[48] Notice to the media does not have to be concurrent with notice to individuals, which provides time to notify individuals before making the breach public.

Business associates: when to delegate

The covered entity is ultimately responsible for ensuring that all required notifications are provided, but it may delegate the task of providing notice to a business associate responsible for the breach.[49] In allocating notice responsibility, organizations should consider which entity has the relationship with the affected individuals.[50] If the covered entity has the primary relationship (the most common situation), the covered entity likely will want to notify affected individuals. When a business associate's breach affects numerous covered entities, it might

45 *Id.* § 164.406(a).
46 78 Fed. Reg. at 5653.
47 *Id.*
48 45 C.F.R. § 164.406(c).
49 78 Fed. Reg. at 5650.
50 *Id.* at 5651.

be preferable for the business associate to provide the notice, so that affected individuals receive just one notification. This might occur, for example, in the context of a health information exchange where the breach compromises a repository that contains the PHI of several covered entities.

Obtaining law enforcement delay if necessary

Both covered entities and business associates may delay required notifications at the request of law enforcement, if giving notice would interfere with a criminal investigation or harm national security.[51] If the request is in writing and specifies a time period, the covered entity or business associate must delay notice for that period.[52] If the request is verbal, the covered entity or business associate may delay notice for no more than 30 days and must document the request and the identity of the requesting official.[53] Organizations should ask law enforcement to provide a written request and retain all documentation so they can demonstrate to the OCR that notifications were timely.

Organizations should also be prepared to explain to law enforcement why a delay would benefit the agency's investigation, and not just the organization. Until law enforcement requests a delay, organizations should proceed under the assumption that notifications must be made by the default deadlines under HIPAA and state law.

State Breach Reporting Laws

Currently, 47 states—as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands—have laws that require reporting of certain breaches involving personally identifiable information. (As of this writing, Alabama, New Mexico, and South Carolina are the only

51 45 C.F.R. § 164.412.
52 *Id.* § 164.412(a).
53 *Id.* § 164.412(b).

states with no breach reporting laws.)[54] Given the variation in states' breach laws, it is critical to assess an organization's obligations under the laws of each relevant state. State law might, for example, require reporting of breaches of personal information beyond PHI; impose shorter reporting timeframes; require notification of additional entities; and mandate different content in the written notice. There are print and online resources that summarize the various state reporting laws, but those laws can change quickly, so when dealing with a breach, it is important to review primary sources of authority.

Coverage of state laws

Some state laws have limited coverage, applying only to a person or entity that does business in that state.[55] Others apply to any person or entity that holds personal information of that state's residents.[56] An attempt by one state to regulate conduct that occurs outside its borders raises potential legal problems, such as under the due process and dormant commerce clauses of the U.S. Constitution.[57] To the authors' knowledge, no court has determined the constitutionality of state breach statutes that attempt to regulate out-of-state businesses. In addition, some state laws exempt organizations subject to federal regulation, such as covered entities or business associates under HIPAA, or financial institutions subject to the Gramm-Leach-Bliley Act.[58] Most states require notification to only their affected residents, but some states require notice to *all* affected people.[59]

---

54 For the citations to all state breach reporting laws that were in effect as of January 1, 2016, *see Security Breach Notification Laws*, Nat'l Conf. of State Legislatures, Jan. 4, 2016, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx; *see also* Jonathan M. Joseph, AHLA Data Breach Notification Laws: A Fifty State Survey, Second Edition (American Health Lawyers Association 2d ed.).

55 *See, e.g.*, Conn. Gen Stat. § 36a-701b(b)(1).

56 See, *e.g.*, Mass. Gen. Laws ch. 93H, § 3(b).

57 *See, e.g.*, Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 Fed. Comm. L. J. 409, 411 (2014-15), *available at* www.fclj.org/wp-content/uploads/2016/01/67.3.2-Glosson.pdf.

58 *See, e.g.*, Ark. Code § 4-110-106; Wis. Stat. § 134.98(3m).

59 *See, e.g.*, Haw. Rev. Stat. § 487N-2(a); N.H. Rev. Stat. §§ 359-C:20(I)(a); N.C. Gen. Stat. § 75-65(a); Tex. Bus. & Com. Code § 521.053(b).

Notifications

Most states put the burden of notifying affected individuals on the person or entity that owns or leases the data. A person or entity that is simply maintaining the data is generally required only to notify the owner.[60] Some states require reporting to state regulators (generally, the state's attorney general), or the three credit reporting agencies if the breach exceeds a certain size.[61]

States generally require notifications of breaches involving a person's name, in combination with any of the following:

1. social security number;
2. driver's license or state ID card number; or
3. credit card number, debit card number, or financial account number, in combination with any password, security code or access code that would allow access to the account.[62]

Some states require notification for breaches of other types of information, including biometrics, taxpayer ID numbers, birth certificates, and medical information.

Nearly every state has a safe harbor (i.e., reporting is not required) if the personal information was encrypted or redacted.[63] The notable exception is Tennessee, which in 2016 modified its breach statute to eliminate the safe harbor for encrypted information.[64] Some states have harm thresholds for reporting, which generally provide that reporting is not required if the breached entity determines there is no reasonable likelihood of harm to consumers or misuse of personal information.[65]

---

60 *See, e.g.*, Utah Code § 13-44-202(3)(b).
61 *See, e.g.*, Fla. Stat. § 501.171(3) & (5).
62 *See, e.g.*, Del. Code tit. 6, § 12B-101(4).
63 *See, e.g.*, Cal. Civ. Code § 1798.81.5 (d)(1)(A).
64 Tenn. Code § 47-18-2107.
65 *See, e.g.*, Mich. Comp. Laws § 445.72(1); Kan. Stat. § 50-7a01(a).

Many states require reporting "in the most expedient time possible and without unreasonable delay . . . ."[66] Some states have imposed specific time limits.[67] The current shortest time period is under California law, which requires notice of health care breaches within 15 business days.[68] States generally allow a breached entity to delay notifications at the request of law enforcement.[69]

State laws vary significantly when it comes to the content of notices. Some have no requirements, leaving it up to the breached entity,[70] while others mandate specific content.[71] Still others *prohibit* certain information in the notices to individuals. Massachusetts forbids including information about the nature of the breach, and both Massachusetts and Illinois bar entities from disclosing the number of people affected.[72] For breaches of unsecured PHI subject to HIPAA, the restrictions under Massachusetts and Illinois law are likely preempted to the extent they conflict with HIPAA's requirements.[73]

Some states allow email notice under certain circumstances,[74] and most states allow substitute notice (i.e., some combination of email, website posting, and media notice) if the breach exceeds a certain size in terms of cost or number of individuals affected.[75]

Breach Prevention and Preparation

Due to the significant likelihood that any given organization will experience a data breach, preparation is critical. One study found that improvements in data governance (such as incident response plans, appointing a chief information security officer, and employee training

66 *See, e.g.*, Ga. Code § 10-1-912(a).
67 *See, e.g.*, Fla. Stat. § 501.171(4)(d).
68 Cal. Health & Safety Code § 1280.15(b).
69 *See, e.g.*, Conn. Gen Stat. § 36a-701b(d).
70 *See, e.g.*, Idaho Code § 28-51-105.
71 *See, e.g.*, Md. Code Com. Law § 14-3504(g).
72 Mass. Gen. Laws ch. 93H, §3(a); 815 Ill. Comp. Stat. 530/10(a).
73 *See* 45 C.F.R. § 160.203 (HIPAA's preemption provision).
74 *See, e.g.*, La. Stat. § 51:3074(E).
75 *See, e.g.*, Minn. Stat. § 325E.61(g).

and awareness programs) and investments in technological solutions (e.g., data loss prevention software, encryption, and endpoint security) significantly reduce the costs of a data breach.[76]

Have an up-to-date security risk analysis and risk management plan

Conducting an in-depth inventory of the organization's data (type of data, where it resides, who has access) and analyzing the risks to that data constitute the basic building blocks of a good security program. The HIPAA Security Rule requires covered entities and business associates to have a current security risk analysis that is "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization] . . . ."[77]

Guidance to help organizations perform a risk assessment is available from the OCR,[78] the Centers for Medicare and Medicaid Services (CMS),[79] the Office of the National Coordinator for Health Information Technology (in partnership with the OCR),[80] and the National Institute of Standards and Technology.[81]

After the risk analysis is complete, the next step is to create and put into practice a risk management plan. The HIPAA Security Rule states that entities must "[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level . . . ."[82]

---

76 2016 Cost of Data Breach Study, at 2.
77 45 C.F.R. § 164.308(a)(1)(ii)(A).
78 OCR, *Final Guidance on Risk Analysis*, HHS.gov, www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html (last visited Nov. 20, 2016) [hereinafter *Final Guidance on Risk Analysis*].
79 CMS, *6 Basics of Risk Analysis and Risk Management*, 2 HIPAA Security Series (2007), *available at* www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf [hereinafter HIPAA Security Series].
80 *Security Risk Assessment Tool*, HealthIT.gov, www.healthit.gov/providers-professionals/security-risk-assessment-tool (last updated Oct. 13, 2016).
81 Nat'l Inst. of Standards & Tech., *Cybersecurity Framework*, www.nist.gov/cyberframework (last visited Nov. 20, 2016).
82 45 C.F.R. § 164.308(a)(1)(ii)(B).

CMS published guidance on implementing a risk management plan.[83] A written risk management plan should address the gaps identified in the risk analysis, include specific tasks to address those gaps, create a timeline, and identify the person responsible for each task.

The security risk analysis and risk management plan should be reviewed and updated periodically and every time there is a material change to the organization's security environment.[84] According to the OCR, "if the covered entity has experienced a security incident, has had change in ownership, turnover in key staff or management, is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI is reasonably and appropriately protected."[85] Health care organizations should integrate the process for updating the security risk analysis and risk management plan into a written information security program.

Implement a written information security program

It is standard business practice to have a written information security program (WISP) that "documents the measures that a business, or organization, takes to protect the security, confidentiality, integrity, and availability of the personal information and other sensitive information it collects, creates, uses, and maintains . . . ."[86] The organization's risk management plan can be included in the WISP. Sample WISPs are available for free online, providing a useful starting point for health care organizations looking to develop their own.[87]

---

83 *Final Guidance on Risk Analysis*; HIPAA Security Series.
84 45 C.F.R. §§ 164.306(e), .316(b)(2)(iii).
85 OCR, *Guidance on Risk Analysis*, HHS.gov, www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Nov. 20, 2016).
86 Melissa Krasnow, Written Information Security Program (WISP), Practical Law, at 1, *available at* https://iapp.org/media/pdf/resource_center/Krasnow_model_WISP.pdf [hereinafter Written Information Security Program].
87 *See* Written Information Security Program; Commonwealth of Mass., Office of Consumer Affairs & Bus. Regulation, A Small Business Guide: Formulating a Comprehensive Written Information Security Program, *available at* www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf [hereinafter A Small Business Guide].

Although the HIPAA Security Rule does not use the term WISP, that is effectively what the Rule requires. Under the Security Rule, both covered entities and business associates must "[i]mplement reasonable and appropriate policies and procedures to comply with [the requirements of the Security Rule]."[88] Those requirements include taking steps to "[e]nsure the confidentiality, integrity, and availability of all electronic PHI [ePHI]," and to protect against "reasonably anticipated" threats, hazards, or unauthorized uses or disclosures of ePHI.[89]

The content of a WISP depends on the nature and size of the business. WISPs for health care organizations generally should include:[90]

- Administrative, technical, and physical safeguards to keep information secure
- A process to identify, on a periodic basis, internal and external threats to information
- A process to manage identified threats
- The identity of the specific employee responsible for maintaining and implementing security policies
- Description of the types of sensitive information maintained by the organization
- Where and how sensitive information is stored
- How sensitive information may be transferred out of the organization
- Procedures for:

  –Username and password assignment

list continues

88 45 C.F.R. § 164.316(a).
89 *Id.* § 164.306(a)(1).
90 *See* Written Information Security Program; A Small Business Guide; Jena Valdetero & David Zetoony, Wash. Legal Found., Data Security Breaches: Incident Preparedness and Response 16–17 (2014), *available at* www.bryancave.com/images/content/2/2/v2/2285/DataBreach-HandbookValdeteroandZetoony.pdf [hereinafter Data Security Breaches: Incident Preparedness and Response].

  - –Password strength and periodic changes
  - –Encryption, including which devices and data must be encrypted, and encryption standards for data in transit and data at rest
  - –Granting and de-activating user credentials
  - –Employee training on security
  - –Destroying data
  - –Retaining vendors that will have access to sensitive data
  - –Disciplinary measures for security violations
- A process for regularly reviewing and updating the program, including the identity of the person responsible

Adopt safeguards to prevent breaches

A few safeguards deserve discussion because they can prevent many data breaches.[91] First, organizations should encrypt devices (especially mobile devices) and data where practicable to take advantage of the reporting "safe harbor" under HIPAA and many state reporting laws. A 2016 study of data breaches showed that encryption reduced the cost of a data breach by $13 per compromised record.[92]

Organizations should consider investing in robust electronic logging features. Logging might help an organization prove that a security incident did not lead to actual exfiltration (removal) of data, allowing it to avoid the substantial cost associated with breach reporting. Special attention should be paid to logging during any transition to new software, which can create gaps in log coverage that compromise subsequent forensic investigations.

---

91 *See generally* FTC, Start with Security: A Guide for Business: Lessons Learned from FTC Cases (2015), *available at* www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

92 2016 Cost of Data Breach Study, at 14.

Health care organizations should take measures to protect passwords, prohibiting employees from using the same password for work and personal accounts, mandating strong passwords through a combination of policies and technology, prohibiting employees from storing passwords near computers or devices, and prohibiting personnel from sharing passwords with others.

Finally, organizations should limit information collected and retain only data that is needed. Regularly reviewing and implementing data-destruction policies will help secure devices and systems no longer in use. Organizations should limit employees' access to only the electronic files, paper documents, and physical locations necessary for their jobs. There should be a process to revisit employees' access when they change roles, and to remove access when they leave the organization.

Train employees on preventing, recognizing, and reporting breaches

One 2016 study of health care organizations found: "While external threats dominate, internal problems such as mistakes—unintentional employee actions, third-party snafus, and stolen computing devices—are equally a problem and account for a significant percentage of data breaches. In fact, 36% of healthcare organizations and 55% of BAs named unintentional employee action as a breach cause."[93] A 2016 study of data breaches showed that employee training on information security reduced the cost of a data breach by $9 per compromised record.[94]

---

93 Ponemon Inst., Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data 1, 2 (2016), *available at* www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm_source=Referral&utm_medium=press%20release&utm_campaign=Ponemon%202016 [hereinafter Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data]; *see also* Verizon, 2016 Data Breach Investigations Report 20 ("63% of confirmed data breaches involved weak, default or stolen passwords"), *available at* www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf; Dan Munro, *Data Breaches In Healthcare Totaled Over 112 Million Records In 2015*, Forbes (Dec. 31, 2015, 9:11 PM), www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-health care-total-over-112-million-records-in-2015/#1fd6afb47fd5 ("[P]eople are still often the weakest link in the security equation. The truth is that it doesn't matter how strong your security is, people still need to be trained properly on how to protect data.").

94 2016 Cost of Data Breach Study, at 14.

Organizations need to train personnel on privacy and security[95] when they are first hired and at least annually after. Training should include information about the organization's privacy and security policies, including the WISP, incident response plan, and breach response plan (if it is not part of the incident response plan), as well as practical information about who to contact if an employee suspects a breach or has questions. Personnel should be reminded that violations of privacy and security policies can lead to employee discipline, as well as other real and personal consequences, such as when the direct-deposit paychecks of a university professor were rerouted by hackers.[96]

Employee training should include information about good security hygiene. Entities should also consider providing ongoing regular privacy and security education and reminders outside of formal training, such as emailing monthly privacy and security tips to all personnel and sharing free, online security resources.[97]

Adopt and test a breach response plan

Health care organizations should establish a breach response team of internal personnel who can bring in outside experts as necessary. A 2016 study of data breaches showed that having a response team reduced the cost of a data breach by $16 per compromised record.[98] An established breach response team can make the breach response faster, more effective, and less stressful for everyone involved.

A response plan can help employees understand their own roles, the roles of other team members, and what they should do (or not do) when

95 *See* 45 C.F.R. § 164.308(a)(5)(i).
96 Darlene Storm, Opinion, *Hacker Steals Teacher's Direct Deposit Paycheck: University Says Too Bad So Sad*, Computerworld (Feb. 3, 2014, 6:00 AM), www.computerworld.com/article/2475732/cybercrime-hacking/hacker-steals-teacher-s-direct-deposit-paycheck--university-says-too-bad-so-sad.html.
97 *See, e.g.*, MIT Info. Sys. & Tech., *Top Ten Safe Computing Tips*, https://ist.mit.edu/security/tips (last visited Nov. 24, 2016); U.S. Small Bus. Admin., *Top Ten Cybersecurity Tips*, www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips (last visited Nov. 24, 2016).
98 2016 Cost of Data Breach Study, at 14.

responding to a security incident or potential breach. A plan's format and content will depend on the size and nature of the entity, but every plan should be specific and actionable, addressing the following points for investigating a potential breach:[99]

- Define triggering events, such as "security incident" and "breach."
- Identify all members of the incident response team, with 24/7 contact information and alternate team members in case designated members are not available. Most health care organizations choose to include representatives of IT, legal, risk management, operations, marketing/communications, finance, audit, and human resources (if the incident involves employee misconduct or affects employees' personal information).
- Include a plan for covering the normal job responsibilities of the team members who are handling the incident.
- Clarify who is responsible for conducting the investigation and response, including:
  - –The role of each team member.
  - –Who is in charge of each aspect of the incident response.
  - –To whom and when information about the incident should be reported.

list continues

99 *See, e.g.*, Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Div., U.S. Dep't of Justice, Best Practices for Victim Response and Reporting of Cyber Incidents 2–3 (2015), *available at* www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf [hereinafter Best Practices for Victim Response and Reporting of Cyber Incidents]; Data Security Breaches: Incident Preparedness and Response, at 18–20; Incident Response Plan Example, *available at* www.cio.ca.gov/ois/government/library/documents/incident_response_plan_example.doc.

  - –Criteria and timelines for escalating the incident to management.
  - –Who has the authority and responsibility to seek additional personnel or resources.
  - –The role of in-house and/or outside counsel, and the process for maximizing the potential to protect the investigation under the attorney-client privilege and work product doctrine.
- Contain instructions on how to preserve evidence, including preserving electronic evidence in a forensically sound manner.
- Prohibit actions that might compromise the breach response. For example, personnel should not make changes to devices or computer systems without the guidance of a forensic consultant or qualified IT expert. Personnel should not attempt to "hack back" into a third-party system that appears to be the source of a cyber-attack.
- Clarify recordkeeping and documentation requirements, including who is responsible, what must be documented, and how long and where documentation must be retained.
- Include a process for post-incident reports to management and self-assessment.

Response plans should also include the following points for those events that the organization determines constitute a breach:

- The organization's policy on breach reporting. This includes addressing who has the authority to decide whether to notify affected individuals, data owners, regulators, the media, law enforcement, and other third parties (such as organizations that share information about cyber threats).
- An alternative communication process. For example, if investigators do not want the hackers to know the organization is aware of the hacking incident (so that the hackers don't create

additional back doors to the system), organizations might use personal emails and cell phone numbers during the initial parts of the breach investigation.

- Contact information for third parties who will be involved in breach response, such as outside counsel; forensic consultants; call center staffing; law enforcement; and vendors who will perform data clean-up, produce and mail letters, and provide credit monitoring and identity protection services.[100]
- A summary of the entity's contractual reporting obligations, including what types of incidents must be reported, the timeline for reporting, and the name and contact information of the person who must receive the report. (This is especially important to business associates.)

At least once a year, the team members should participate in a tabletop drill where they practice responding to a simulated incident. That will allow team members to get comfortable with their roles and the other team members. It can also help identify areas where the response plan can be improved.

Be proactive with business associates and other vendors

In one 2016 study, 41% of health care organizations reported that they had a breach caused by a third party.[101] An organization needs to look beyond the security of its own information systems and employees and examine vendors who have access to or host the organization's data. That includes billing companies, accountants, attorneys, document storage and shredding companies, and cloud storage providers. Under both HIPAA and state breach laws, organizations are responsible for reporting breaches by third parties in possession of the organizations'

100 Organizations should consider identifying or even contracting with vendors in advance of a breach. It might allow the organization to negotiate better rates.

101 Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, at 2.

PHI or personal information. Breaches by third parties can also lead to lawsuits against the organization, government investigations, and fines.

Organizations can reduce the risk by vetting vendors' privacy and security practices, and putting protective measures in vendor contracts. HIPAA requires covered entities and business associates to enter into written business associate agreements (BAAs), and requires certain content in those agreements.[102] Although HIPAA applies to a covered entity's relationship with only vendors that use or disclose the entity's PHI, the information handling and reporting requirements of a BAA are a good starting point for written agreements with all vendors that will receive sensitive information.

HIPAA does not, however, address all important aspects of the covered entity-BAA relationship, such as financial responsibility for breaches. Organizations should therefore go beyond HIPAA's requirements of a BAA and address the following issues in vendor contracts:[103]

- Specify how to communicate security incidents and breaches:
  - –What types of incidents the vendor must report to the organization. Entities might consider requiring reporting of all suspected security incidents or breaches, so that the vendor is not responsible for determining whether there is a reportable event.
  - –The timeline for vendor reporting. Making the timeline short allows the covered entity more time to conduct an adequate

102 The website of the OCR includes a sample business associate agreement that includes all of the provisions required by HIPAA. U.S. Dep't of Health & Human Servs., *Business Associate Contracts: Sample Business Associate Agreement Provisions*, HHS.GOV (Published Jan. 25, 2013), www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

103 *See generally* AHA, ATTACHMENT TO AHA LEGAL ADVISORY: BUSINESS ASSOCIATE AGREEMENT: A CHECKLIST OF REQUIRED AND OPTIONAL PROVISIONS, *available at* www.aha.org/content/00-10/ChecklistOfReqOptElements092302.pdf; Ober Kaler, PREPARING FOR THE HITECH SEPTEMBER DEADLINE: TIPS FOR NEGOTIATING EFFECTIVE BUSINESS ASSOCIATE AGREEMENTS UNDER HIPAA (July 29, 2014), *available at* www.bakerdonelson.com/2673-webinar-preparing-hitech-september-deadline-tips-negotiating-effective.

investigation or oversee the business associate's investigation. Quick reporting also may help mitigate any potential damages by allowing affected people to promptly obtain identity theft protection services.

–The name and contact information of the representative who should receive the vendor's report, and the information the vendor must include in the report. HIPAA requires certain information for breaches of unsecured PHI,[104] but the entity might want to require a report of the types of PHI or other sensitive information compromised for each individual (if it varies), the last known mailing address of each individual, and the name and contact information for the vendor's point of contact.

- Require the return or destruction of PHI and other sensitive information after the vendor's work is finished. A BAA must allow a vendor to maintain PHI after the conclusion of the work if it is infeasible to return or destroy the information.[105] The agreement should specify whether the covered entity or business associate decides whether it is feasible. To the extent the vendor receives PHI or other sensitive information that is not necessary for the vendor's work (for example, if the covered entity provides information by mistake), the agreement should require destruction of that information promptly (not at the end of the agreement).
- Require the vendor to cooperate with the entity's investigation of an incident or breach, including providing updates from the vendor's investigation.
- Establish the right to audit the vendor's privacy and security practices, either on a regular basis or upon a breach. The vendor

104 45 C.F.R. § 164.410(c).
105 *Id.* § 164.504(e)(2)(ii)(J).

should be required to have a WISP and incident response plan. Many organizations have created robust screening requirements to confirm that vendors' security requirements are sufficient.

- Specify and require safeguards relevant to the context. For example, depending on the service, the entity may want 24/7 video surveillance of sensitive areas, specific password requirements, or encryption of portable devices. Entities should consider requiring representations and warranties that the vendor has performed background checks on all personnel who might work with the covered entity's data.
- Include terms regarding liability for the costs of a breach. The agreement should address whether the business associate is responsible for:
  - –All of the covered entity's direct costs (e.g., forensic consultant, attorneys, and mailing).
  - –The covered entity's indirect costs (employee time in responding to the breach, lost business).
  - –The cost of all services offered to individuals, including those that are not legally required.
- Include terms regarding control of the notification process. In general, covered entities will want exclusive control of the content of notices. Business associates will want a voice in the process to prevent the covered entity from shifting blame unfairly and to keep costs down. The contract should establish:
  - –Who decides whether to notify individuals, government regulators, the media, and other third parties.
  - –Who controls the content of the notices.
  - –Who decides which vendors to retain (e.g., forensic consultant, attorneys, mailing, call center, credit monitoring and identity theft protection services).

list continues

–Who decides which products and services to offer affected individuals.

- Address indemnification. Will the vendor indemnify the entity for all damages arising from the breach, regardless of fault? Or will indemnity be limited to harm caused by the vendor's acts or omissions, or some fault standard (e.g., negligence, recklessness, intentional misconduct)? Covered entities will want very broad indemnification, while business associates will want to take on the minimum possible responsibility.
- Require the vendor to carry cyber insurance sufficient to cover the vendor's indemnification obligations. Consider including requirements regarding the scope of coverage, including the per-incident and aggregate dollar limits.

Establish relationships with organizations that share information on cyber threats

Sharing information about cyber threats can help organizations prioritize their security measures and stay on top of the latest trends and risks. Organizations that have multiple locations (such as hospital systems) need processes to make sure that information about cyber incidents and threats is shared among different locations.

One information-sharing group that might be helpful to health care organizations is the National Health Information Sharing and Analysis Center.[106] Its members are "primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities . . . advice and best practices, mitigation strategies and other valuable material."[107] A 2016 study showed

106 *National Health Information Sharing and Analysis Center*, Nat'l Health–ISAC, www.nhisac.org/ (last visited Nov. 26, 2016).
107 *Id.*, https://nhisac.org/about-nhisac/.

that "participation in threat sharing" reduced the cost of a data breach by $9 per compromised record.[108]

Ensure adequate cyber insurance coverage

Every organization that handles PHI or other sensitive personal information should obtain cyber insurance. Cyber policies vary significantly in terms of the types of incidents they cover, their exclusions, and the coverage amounts. When seeking cyber coverage, organizations should work with a knowledgeable insurance broker or experienced attorney. This is an area where both the law and current risks change quickly, so organizations should review their cyber coverage at least annually.

Legal counsel and other appropriate organizational representatives (such as risk management and members of the incident response team) should review the cyber policy before a security incident or breach. Some insurance policies require organizations to follow minimum security standards, and the organization will need to know the policy's requirements for giving notice and cooperating with the insurer. Policies might also require the use of pre-approved vendors, such as for legal services, forensic consulting, mailing, and call center staffing.

Responding to a Breach

The first step in responding to a breach is convening the team that will lead the response. Ideally, this will be the team identified in the incident response plan. If the entity does not have an incident response plan, it should form a committee of high-level personnel with the expertise and authority to command immediate action.

The response team should assign one member the responsibility of documenting all steps of the investigation and response, including the dates and times of all significant events, and the identity of every person involved in the process. It is much easier to document actions as they

108 2016 Cost of Data Breach Study, at14.

happen, rather than trying to reconstruct them months or years later for a government investigation or litigation. The documentation should stick to verifiable facts and avoid speculation or opinion.

Address attorney-client privilege and work product protection

An incident investigation might reveal information that could be harmful to the entity if it were disclosed publicly, such as technical vulnerabilities in the entity's computer systems. Many entities therefore choose to have attorneys direct the incident response to protect as much information as possible under the attorney-client privilege and work product doctrine.

If attorneys will direct the incident response, they should retain any forensic investigators directly. The retention agreement should note that the attorneys are engaging the forensic investigators for the purpose of facilitating legal advice to the client (the covered entity or business associate). An attorney should be involved in all communications between the forensic investigators and the client. The forensic investigators should provide drafts of their report to the attorneys for review and approval. As part of that process, counsel should make sure that the report is complete and accurate and does not contain inaccurate information, speculation, or irrelevant details that might be harmful to the client if the report were disclosed to a third party, such as in a government investigation or litigation.

Instruct personnel to keep information about the breach confidential

The incident response team should strive to keep information about the breach from becoming public until the organization has decided to report it. To minimize the spread of information, the response team should specifically direct every employee who has information about the breach to keep it confidential and not discuss it with anyone unless authorized by the appropriate authority from the response team or management.

Retain a computer forensic consultant

A forensic consultant can, among other things, help stop an ongoing attack, identify compromised data and systems, and delete malware and other hacker tools from the system. Critically, a qualified forensic expert can preserve digital evidence in case it is needed for a criminal case, civil litigation, or government investigation. If legal counsel is directing the investigation, counsel should retain the forensic consultant so that the consultant's report is privileged.

Preserve evidence

The entity must retain all information potentially relevant to government investigations or litigation arising from the breach. Depending on the type of breach, the entity might need to make forensic copies of all affected devices and systems, obtain and store electronic logs, preserve video camera footage, or save emails or other communications. The forensic consultant should lead this process and make sure all relevant digital evidence is preserved. The organization's personnel should not try to conduct any electronic investigation except under the supervision and direction of the forensic consultant (or other qualified IT personnel) to avoid destroying evidence inadvertently.

Depending on the size and nature of the breach, the organization might also need to—under the guidance of legal counsel—issue a document-preservation notice to prevent the organization's employees from destroying potentially relevant materials.

Control the damage

The entity should take whatever steps are necessary to stop the incident (if it is ongoing) and prevent or at least minimize additional harm. That might involve removing affected devices from the network, shutting off unauthorized access to the system, placing physical security devices such as locks on sensitive areas, or suspending or terminating an employee

suspected of participating in a breach. Any actions involving computer systems should be done at the direction, and under the supervision, of a highly qualified technical expert. Organizations should consider whether they have the in-house IT expertise necessary to respond to a security event. For smaller or less technically savvy organizations, it often makes sense to engage an outside breach-management vendor.

Decide whether to contact law enforcement

A health care organization must balance the potential benefits of contacting law enforcement with the risk of losing control over the investigation. For most breaches, there is no reason to report to law enforcement. Getting law enforcement involved makes sense, however, when the person or people responsible for the breach should be held accountable, or where the government's powers of investigation (such as the ability to obtain subpoenas and search warrants) would be helpful. Another reason to contact law enforcement is to try to get a request to delay notifications, as explained earlier.

Incidents that involve the exfiltration (removal) of data from a computer system can be reported to either the FBI's cybercrimes unit or to the U.S. Secret Service. Breaches that involve paper records or known perpetrators (such as employees) can be reported to the local police department.

The cybersecurity unit of the U.S. Department of Justice (DOJ) also recommends that organizations consider contacting the National Cybersecurity & Communications Integration Center (NCCIC), which is available 24/7. According to the DOJ's cybersecurity unit, "By contacting the NCCIC, a victim organization can both share and receive information about an ongoing incident that may prove beneficial to both the victim organization and the government. A victim organization may also obtain technical assistance capable of mitigating an ongoing cyber incident."[109]

109 Best Practices for Victim Response and Reporting of Cyber Incidents, at 11–12.

Interview personnel

Members of the incident response team should document key facts and interview everyone who has information about the incident as soon as possible, before memories fade and key documents are lost. If the investigation is being led by counsel, an attorney should participate in the interviews and in drafting written summaries of them. To maximize the chances of protection under the work product doctrine, written summaries should include the observations, opinions, and thoughts of the attorney, as opposed to verbatim transcripts of the witnesses' statements.[110]

Notify insurance carriers

The entity should immediately notify all insurers whose policies might provide coverage for the incident, including cyber insurance, commercial general liability, professional liability, errors and omissions, and other types of policies. Insurance policies generally require prompt notice and cooperation with the insurer's protocols and claim investigation.

Decide whether to report the breach

The entity must determine whether it has a legal obligation to report under HIPAA and state laws. It should also determine whether it has contractual obligations to report the breach under BAAs or other contracts.

Prepare for communications with media and other third parties

In addition to drafting any media notice required by HIPAA or other law, the organization should proactively prepare to respond to questions about the breach from the media and other third parties, such

110 *See* Upjohn Co. v. United States, 449 U.S. 383, 401–02 (1981) (discussing the very significant showing of necessity that is required for disclosure of materials that reveals an attorney's mental processes); Fed. R. Civ. P. 26(b)(3)(B).

as patients, customers, and business partners. Depending on the size and nature of the breach, the organization should consider retaining a public relations firm that has experience dealing with data breaches. The firm may have personal contacts within the media, which could help de-sensationalize reporting. A public relations firm will also be trained in clear, concise communication and can help avoid "legalese" in the notices.

Draft notices

Legal counsel should participate in the drafting to make sure notices comply with all legal requirements and minimize the possibility that the notices might harm the organization during a later government investigation or litigation. An employee or outside consultant with experience in communications or public relations should also participate, if possible. The notices should be approved by the appropriate representative(s) of the organization (who ideally will be specified in the incident response plan and/or breach reporting policy).

Decide what services to offer affected individuals

There is generally no legal requirement to provide credit monitoring or identity theft protection services, although California requires any entity that chooses to provide identity theft protection and mitigation services to provide them for at least 12 months.[111] Entities generally offer these services to individuals for 1–3 years,[112] and should carefully screen the vendors that provide these services. In previous breaches, vendors

111 Cal. Civ. Code § 1798.82(d)(2).

112 *See* Dep't of the Navy, Frequently Asked Questions: OPM Data Breach 4 (2015), *available at* www.secnav.navy.mil/OPMBreachDON/Documents/2015/09/DON_OPM_Breach_FAQs_091515.pdf (noting that the federal government had offered either 18 months or 3 years of ID theft protection services to people affected by two different incidents); Michael Hiltzik, *Anthem is Warning Consumers About its Huge Data Breach. Here's a Translation*., L.A. Times (Mar. 6, 2015, 10:34 AM), www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html (noting that Anthem offered 2 years of ID theft protection).

have been criticized for providing false or misleading information to consumers, or for trying to upsell more expensive services to affected individuals. Entities must also assess what information the vendor will need to implement the services offered (i.e., whether the vendor needs individuals' information in advance to issue registration codes).

Make logistical arrangements

For breaches of any significant size, the logistics of notifications can require a significant amount of time and resources. It is important to start thinking about them early in the process. Depending on what notifications and services the organization has decided to provide, it needs to make arrangements for either its personnel or outside vendors to:

- Compile a spreadsheet of all the names, addresses, and types of PHI compromised for all affected individuals (making sure to remove duplicate names). For very large breaches, the entity might have to hire outside consulting help to assist in understanding which individuals have been affected and de-duplicating the contact information.
- Prepare, print, and mail letters for individual notices. It takes a substantial amount of time to print and stuff envelopes for breaches involving hundreds of thousands or millions of individuals.
- Run all individuals' addresses through the U.S. Postal Service's change-of-address database. That will reduce the amount of returned mail and might allow the entity to send the letters first class (as required by HIPAA) but at the bulk mail rate.
- Determine who will handle calls from individuals who have questions or want to activate any offered credit monitoring or identity theft services. For significant breaches, this is usu-

ally outsourced to a call center. We recommend that the entity provide a script to the call center with responses to FAQs and a process for escalating calls to a representative of the breached entity. The entity should closely examine whether the call center has the capacity to handle the anticipated call volume, including its back-up procedures in case call volume is greater than expected.

Document all steps of the breach response

Proper documentation is required by HIPAA and is a best practice for all types of breaches. Under HIPAA, a covered entity or business associate must maintain documentation demonstrating either that the organization made all required notifications or that notification was not required.[113] HIPAA also requires covered entities and business associates to develop and document policies and procedures governing breach incidents and to retain in writing, for a period of six years, policies and procedures and any other activity (e.g., employee sanctions) that must be documented.[114]

Adopt and implement a corrective action plan

After an organization determines that an incident is a reportable breach, the organization should focus on mitigation and documenting a corrective action plan. Key areas to focus on when taking corrective action are:

- Mitigating the risk to individuals affected by the breach.
- Addressing the systemic problems that created the breach. For example, if the breach involved the loss of an unencrypted

113 45 C.F.R. § 164.414(b); 78 Fed. Reg. 5566, 5657–58.
114 45 C.F.R. § 164.414(a); 78 Fed. Reg. at 5657.

laptop, the organization should implement a program for encrypting all laptops and other portable media.

- Implementing appropriate discipline for the personnel who caused the breach (consistent with the organization's personnel policies).
- Providing additional training. This should include training on any systemic fixes to address the breach, policy changes, and other information that will be relevant to the organization's personnel.

Organizations should start corrective actions as soon as possible. HIPAA provides an affirmative defense to civil money penalties for breaches that were not due to willful misconduct and are corrected during "[t]he 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred . . . ."[115] All corrective actions should be documented, and the organization should retain such documentation for at least six years.[116]

Perform or update the security risk analysis

After a breach, organizations should update their security risk analysis and risk management plan. If an organization has not undergone a security risk analysis, it should perform one right away and start implementing a risk management plan. In the authors' experience, OCR investigators routinely ask for a copy of the organization's risk analysis at the beginning of an investigation.

115 45 C.F.R. § 160.410(c)(2)(i).
116 *Id.* § 164.316(b).

Conclusion

Data breaches are now a reality of doing business, particularly for health care organizations. Appropriate prevention can reduce the likelihood of a breach, and preparation can reduce the associated costs. However, the health care industry and its regulators should take a long and hard look at whether the present breach-reporting requirements should be changed. Dealing with a large data breach is incredibly expensive, especially for many community hospitals and physician groups that operate on a thin profit margin. It is debatable whether notice to individuals makes a difference in the majority of instances where reporting is required. People are weary of data breaches and often do not bother to sign up for any offered credit monitoring or identity theft resolution services.

Perhaps a wiser path would be to institute individual authentication requirements for obtaining credit and other services, so that identity thieves could not use the breached data for those purposes. Another option would be for CMS and other payers to institute smarter algorithms to catch fraudulent claims. Ultimately, what would help consumers most is a system that requires reporting to individuals who must know about the breach in order to protect themselves. Modifying the reporting requirements to provide real protection to individuals in a manner that is less financially burdensome to the health care industry would benefit everyone.