Data Breach Risks and Best Practices for Small and Mid-Size Health Care Providers[1]

By: Michael J. Waters, Ethan E. Rii and Joshua J. Orewiler

Edited by: Louis C. Szura

[1] This publication is intended to serve as a preliminary research tool for attorneys for educational purposes only. It should not be used as the sole basis for making critical business or legal decisions. This publication does not constitute, and should not be relied upon as, legal advice.

TABLE OF CONTENTS

I. Introduction

In recent years, the likelihood of suffering a data breach has risen significantly for American companies across numerous industries. Health care providers, in particular, have been targeted due to the value of the sensitive information they hold regarding their patients and employees, including birth dates and Social Security numbers.[i] Health care providers that suffer data breaches risk incurring significant fines, settlement amounts, legal fees, negative publicity and increased scrutiny from regulatory authorities.

Several recent breaches involving health care providers have resulted in very large monetary penalties and settlements with the U.S. Department of Health & Human Services (HHS), Office for Civil Rights (OCR). For example, Cancer Care Group, P.C. recently entered into a settlement with OCR for $750,000 relating to a breach caused by the theft from an employee's vehicle of computer server backup media containing unencrypted electronic protected health information (ePHI) of approximately 55,000 individuals.[ii] In addition, Lahey Hospital and Medical Center (Lahey) recently agreed to an $850,000 settlement with OCR relating to the theft of an unencrypted laptop that contained ePHI of 599 individuals from an unlocked room in Lahey's Radiology Department.[iii]

Given the risk for substantial fines and penalties from data breaches affecting a relatively small number of individuals, health care providers should (i) devote the necessary time and resources to comply with privacy regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, (ii) implement policies and procedures to reduce their risk of data breaches, and (iii) prepare for responding to the inevitable data breach.

II. Recent Data Breach Trends for Health Care Providers

According to a recent study, ninety-six percent (96%) of HIPAA covered entities[iv] have suffered a security incident involving a lost or stolen device.[v] A significant majority of those covered entities have experienced security incidents from spear-phishing and web-borne malware attacks.[vi] In total, ninety-one percent (91%) of covered entities suffered a data breach within the last two years.[vii] In addition, forty percent (40%) of covered entities suffered more than five data breaches within the last two years, while an additional thirty-nine percent (39%) suffered two to five data breaches within the last two years.[viii]

Within the health care profession, small and mid-size health care providers are more vulnerable to data breaches due to the limited resources and manpower that they have available to implement, maintain and enforce internal policies and procedures to protect and safeguard protected health information (PHI). Typically, a data breach affecting a mid-size health care provider will involve the health care provider having to notify individuals residing in thirty-five (35) to forty (40) different states. Thus, the health care provider will have to comply with HIPAA breach notification requirements, as well as the notification requirements under the law of each state in which the affected individuals reside.

In addition to the costs of notification obligations to OCR and affected individuals, data breaches can cause significant negative publicity for a health care provider. The negative

publicity of a data breach may cause patients, customers or employees to fear that the health care provider is not capable of sufficiently protecting their personal information or PHI. Further, a health care provider that suffers a data breach must devote significant resources to investigating the breach, including how the breach occurred, what information was affected, whose information was affected, and what steps it must take to notify those individuals and mitigate the harm resulting from the breach. Additionally, data breaches, particularly large breaches involving Social Security numbers, may cause increased scrutiny from regulators at both the state and federal levels. Given the numerous adverse effects that a data breach may have on a health care provider, covered entities and business associates[ix] should ensure that they are taking all reasonable steps to properly protect and safeguard all personal information and PHI.

As discussed later in this article, many recent data breaches involving health care providers have been caused by a failure to encrypt laptop computers and other electronic devices that contained ePHI and were lost or stolen. Under HIPAA regulations, if a laptop or other electronic device containing ePHI is properly encrypted, the loss or theft of that device will generally not constitute a breach requiring notification.[x] HIPAA regulations define encryption as the "use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[xi] While health care providers are not required to encrypt every device containing ePHI, HIPAA regulations require that they conduct a risk assessment to determine whether encryption or some other form of security is necessary to protect ePHI.[xii] It is important to note that while password protecting devices may be helpful, it is usually not sufficient to protect ePHI. The loss by or theft from a heath care provider of a device containing ePHI, when the device is password protected but not encrypted, will generally be considered a breach requiring notification under HIPAA.[xiii]

III. Recent Enforcement Trends against Health Care Providers

A. Potential Monetary Penalties for Health Care Providers that Suffer a Data Breach

Under current regulations, the Secretary of HHS (Secretary) may impose a civil money penalty (CMP) upon a covered entity or business associate for a violation of HIPAA privacy regulations, the amount of which is based upon the knowledge and diligence of the entity in attempting to comply with such regulations.[xiv] The range of CMPs that the Secretary may impose for a particular breach incentivizes health care providers to take reasonable and diligent measures to comply with all HIPAA privacy regulations and to correct any violations as soon as possible. Generally, the potential CMPs vary based on whether the breach could have been prevented using reasonable measures, whether the health care provider made reasonable efforts to comply with HIPAA privacy requirements and whether the health care provider corrected the violation within thirty (30) days after learning of the breach.[xv] Additionally, the regulations provide that the Secretary will consider the following factors in determining the appropriate CMP: (a) the nature and extent of the violation, (b) the nature and extent of harm resulting from the violation, (c) the entity's prior compliance history, (d) the entity's financial condition, and (e) any other factors "as justice may require."[xvi]

The regulations address numerous potential breach scenarios. Generally, the regulations provide that the Secretary must impose a CMP within a certain range that varies based on the knowledge of the covered entity and whether the covered entity timely corrected the violation, unless the covered entity is able to establish an affirmative defense to the violation.[xvii] For a violation with regard to which the entity lacked knowledge, and could not have known by

exercising reasonable diligence, that the violation was occurring, HHS regulations provide that the Secretary may impose a CMP between $100 and $50,000 for each violation.[xviii] Additionally, for violations in which the entity's violation was due to "reasonable cause," which the regulations define as an act or omission that the entity knew, or would have known by exercising reasonable diligence, constituted a violation, the Secretary may impose a CMP between $1,000 and $50,000.[xix] However, the Secretary may not impose a CMP if the violation is corrected within (i) thirty (30) days of when the entity discovered or reasonably should have discovered the violation or (ii) a period longer than thirty (30) days determined by the Secretary to be appropriate based on the nature and extent of the violation.[xx] Further, even if the violation is not corrected within the relevant time period, the Secretary has discretion to waive the CMP, in whole or in part, to the extent that the CMP would be excessive relative to the violation.[xxi]

In addition, for violations resulting from "willful neglect," which the regulations define as the "conscious, intentional failure or reckless indifference to the obligation to comply" with the provision violated, that the entity corrected within thirty (30) days of when it discovered or reasonably should have discovered the violation, the Secretary will impose a CMP between $10,000 and $50,000.[xxii] However, when a violation results from willful neglect and is not corrected within the thirty (30) day period after the entity discovers or reasonably should have discovered the violation, the Secretary must impose a CMP of not less than $50,000.[xxiii] When a violation results from willful neglect, the Secretary does not have discretion to waive or reduce the CMP, regardless of when the violation was corrected or whether the CMP would be excessive relative to the violation. Finally, HHS regulations cap the aggregate amount of penalties that the Secretary may impose upon one entity in a calendar year at $1,500,000.[xxiv]

OCR will routinely conduct an investigation of a health care provider that reports a data breach to OCR. These post-breach investigations essentially function as an informal audit of the health care provider, in which OCR will investigate not only the causes and factors leading to the specific breach reported, but also the provider's compliance with all privacy regulations. OCR will take into account the health care provider's compliance, or lack of compliance, with HIPAA requirements in determining the appropriate CMP or settlement offer to which it will agree. Thus, when a health care provider suffers a data breach, it should expect that OCR will take a close look at its compliance with all of the privacy requirements, not only the specific violation(s) that caused the breach.

B. Examples of Recent Data Breach Settlements with OCR

Cancer Care Group, P.C.

One example of a recent breach that resulted in an investigation by OCR and a large settlement involved Cancer Care Group, P.C. (CCG), a large provider in Indiana focused on treating patients with radiation therapy.[xxv] In July 2012, a CCG employee left his computer and unencrypted backup media in his vehicle.[xxvi] Someone broke into his car and stole the backup media, which contained the PHI of approximately 55,000 individuals.[xxvii]

Following CCG's report of this breach to OCR on August 29, 2012, OCR conducted a full investigation into CCG's compliance with relevant regulations regarding the protection of ePHI.[xxviii] OCR's investigation determined that CCG engaged in the following conduct: (1) improperly disclosing the ePHI of 55,000 individuals by failing to safeguard the unencrypted computer server media backup stolen from the employee's vehicle, (2) failing to

adequately assess the risks to the confidentiality of ePHI held by CCG, and (3) failing to implement proper policies and procedures regarding the removal of hardware and electronic media containing ePHI from its facilities.[xxix]

CCG agreed to a Resolution Agreement that required CCG to pay a settlement amount of $750,000 to OCR.[xxx] In addition, CCG agreed to enter into a three-year Corrective Action Plan (CAP).[xxxi] The CAP requires CCG to (1) conduct a risk analysis into its security risks relating to ePHI, (2) develop and implement a risk management plan to reduce any security risks it identifies, and (3) review and revise its policies, procedures and training program to comply with the HIPAA regulations.[xxxii] In addition, CCG must investigate any information it receives indicating that any of its employees may have failed to comply with the above-mentioned policies and procedures.[xxxiii] If CCG determines that one of its employees failed to comply with these policies and procedures, it must notify OCR within thirty (30) days. Finally, CCG must submit to OCR detailed annual reports regarding CCG's compliance with the CAP.[xxxiv]

Lahey Hospital and Medical Center

Similarly, Lahey Hospital and Medical Center (Lahey) recently agreed to a settlement with OCR that required Lahey to pay $850,000 as the result of the theft of an unencrypted laptop.[xxxv] The laptop had been used with a computerized tomography scanner and, consequently contained the ePHI of 599 individuals.[xxxvi] It was stolen from an unlocked room in Lahey's Radiology Department. OCR conducted an investigation following Lahey's report of this breach and determined that Lahey violated numerous regulations relating to the safeguarding of ePHI, including: (1) impermissibly disclosing the ePHI of 599 individuals, (2) failing to conduct an adequate analysis of risks to the confidentiality of ePHI, (3) failing to implement reasonable physical safeguards to restrict the access of unauthorized users to a workstation capable of accessing ePHI, (4) failing to implement proper policies and procedures governing the removal from its facility of hardware and electronic media containing ePHI, (5) failing to create a unique user name to identify and track user identity on the relevant workstation, and (6) failing to implement mechanisms to record activity on the relevant workstation.[xxxvii]

As a result of the breach and OCR's investigation, Lahey also entered into a CAP with OCR, which, similar to the CAP in CCG's case, required Lahey to conduct a risk analysis relating to risks associated with the ePHI on its electronic media, workstations and information systems.[xxxviii] Lahey was also required to create written policies and procedures to remedy its failure to comply with regulatory requirements.[xxxix] Additional provisions of Lahey's CAP require Lahey to properly train all employees who may access ePHI and to investigate any potential failure to comply with its above-mentioned policies and procedures and report any such lack of compliance to OCR.[xl] Finally, Lahey must submit a detailed implementation report describing how Lahey complied with the terms of the CAP and must provide an attestation of the facts in the report that is signed by an officer of Lahey.[xli]

Other Examples

Several other recent breaches involving the theft of unencrypted laptops from health care providers, or their workforce members, have resulted in significant settlements with OCR. In November 2011, an unencrypted laptop containing ePHI was stolen from a physical therapy center of Concentra Health Services (Concentra).[xlii] After OCR conducted its typical data breach investigation, it found that Concentra had failed to properly encrypt numerous laptops containing

ePHI over the time period from October 2008 until June 2012.[xliii] To settle the alleged violations with OCR, Concentra agreed to pay a settlement amount of $1,725,220 and to enter into a CAP.[xliv]

Similarly, QCA Health Plan, Inc. of Arkansas (QCA) agreed to pay a settlement of $250,000 as a result of the theft from a workforce member's car of an unencrypted laptop that contained the ePHI of 148 individuals.[xlv] Following notification of the breach, OCR investigated QCA and determined that QCA violated the HIPAA Privacy and Security Rules in several ways, including the failure to develop and implement proper policies and procedures to prevent security violations.[xlvi] Those alleged failures led to the large settlement.

These recent data breach settlements demonstrate a trend of OCR requiring significant settlement amounts from health care providers who fail to properly encrypt laptops containing ePHI, or otherwise adequately safeguard such information, even for a small group of individuals. Prior to December 2012, OCR had not entered into a settlement agreement for a breach involving unsecured ePHI of fewer than 500 individuals.[xlvii] In December 2012, however, OCR agreed to settle alleged HIPAA violations by The Hospice of North Idaho (HONI) for an amount of $50,000, plus HONI's agreement to implement and follow a CAP.[xlviii] The breach in that case resulted from the theft of an unencrypted laptop that contained the ePHI of 441 patients.[xlix] However, as the more recent breaches indicate, OCR is increasingly pursuing larger settlement amounts for breaches involving ePHI. In light of this trend, small and mid-size health care providers should ensure that they are implementing and enforcing policies and procedures to encrypt all forms of electronic media containing PHI.

However, not all data breaches involve unencrypted laptops or even ePHI. For example, in March 2015, Cornell Prescription Pharmacy (Cornell) agreed to pay $125,000 to settle allegations that it disposed of unsecured physical documents containing the PHI of 1,610 patients in an unlocked, open container on its premises.[l] Similar to breaches involving ePHI, OCR conducted an investigation into Cornell's compliance with HIPAA regulations and found that Cornell had committed several violations.[li] Given the significant settlement paid by Cornell, and its agreement to enter into a CAP, all health care providers, regardless of their size, should ensure that they properly protect and dispose of both paper and electronic records containing PHI.

C. Examples of Recent Data Breach Settlements with State Attorneys General

Health care providers that have suffered data breaches involving the loss of unencrypted ePHI also have settled claims with applicable state Attorneys General. For example, in November 2014, Beth Israel Deaconess Medical Center, Inc. (Beth Israel) agreed to a $100,000 settlement with the Office of the Attorney General of the Commonwealth of Massachusetts.[lii] The breach at issue in that case involved a physician's laptop containing ePHI and Social Security numbers of 3,796 individuals that was stolen from an unlocked office.[liii] While Beth Israel had a policy requiring its employees to encrypt and physically secure all laptops containing ePHI or personal information, the physician and other employees of Beth Israel were not following this policy.[liv] In addition to the $100,000 settlement, Beth Israel agreed to take steps to prevent similar future breaches, including implementing and enforcing policies requiring all laptops containing ePHI to be encrypted.[lv]

While the Beth Israel case involved a health care provider located in the same state as the Attorney General's Office, a state Attorney General is not limited to enforcing its privacy laws and regulations against health care providers located in its state. Under certain states' laws, a state Attorney General may bring an enforcement action against a health care provider, regardless of where the provider is located, when that provider's failure to follow privacy laws or regulations results in a breach affecting an individual who resides in that state. In July 2014, the Attorney General of Massachusetts settled allegations against the Women & Infants Hospital of Rhode Island (WIH) that WIH violated privacy laws and regulations as a result of WIH's loss of nineteen (19) backup tapes from two prenatal centers.[lvi] The misplaced tapes contained ePHI and personal information, including Social Security numbers, of 12,127 Massachusetts residents and approximately 1,200 Rhode Island residents.[lvii] To settle this breach with the Massachusetts Attorney General's Office, WIH agreed to pay a total of $150,000 and to implement policies to prevent future breaches, including maintaining an inventory of all unencrypted electronic media containing personal information and PHI.[lviii]

D. Potential Liability from Civil Lawsuits as a Result of a Data Breach

HIPAA does not create a private cause of action for individuals whose PHI is compromised by a breach. However, individuals whose personal information or PHI has been compromised have sought relief based on numerous theories of liability, including negligence in allowing the breach, fraud in misrepresenting privacy or security policies, breach of contract, failure to comply with state data breach notification requirements, unjust enrichment, statutory claims under the Stored Communications Act, Electronic Communications Privacy Act or Computer Fraud and Abuse Act, and securities and shareholder derivative suits. A common theme in those cases is whether there is a case or controversy that affords the plaintiff standing under Article III of the United States Constitution to bring such claims. In many cases, courts have dismissed claims based on data breaches when the plaintiff alleged that his or her personal information or PHI was stolen, but did not allege that he or she had suffered from actual identity theft.[lix] In those cases, many courts have held that a plaintiff's personal information or PHI being compromised was not in itself sufficient to confer Article III standing upon the plaintiff.[lx] A minority of cases, however, have held that the increased risk of identity theft arising out of a plaintiff's personal information or PHI being compromised is sufficient to meet the injury-in-fact requirement for Article III standing.[lxi]

Despite the fact that data breach lawsuits may be dismissed in the early stages, recent settlements indicate that breaches by health care providers have the potential to lead to substantial liability. For example, in 2013, AvMed Inc. agreed to a $3 million settlement based on a data breach caused by a laptop stolen in 2009 that contained the personal information of approximately 1.2 million of AvMed's customers.[lxii] In particular, this settlement allowed plaintiffs who did not experience identity theft to recover money from the $3 million settlement fund.[lxiii] Similarly, in 2014, a $4.1 million settlement was approved in a data breach lawsuit alleging that Stanford Hospital & Clinics and its billing subcontractor Multi-Specialty Collection Services, LLC allowed approximately 19,500 Stanford patients' names, account numbers and diagnoses to be visible on a publicly available website.[lxiv] These recent settlements demonstrate that data breaches, and the resulting lawsuits, may create significant civil liability for health care providers.

IV. Data Breach Notification Obligations under HIPAA/HITECH Act

Under federal regulations promulgated by HHS pursuant to HIPAA and the HITECH Act, a covered entity has a duty to notify every individual "whose unsecured [PHI] has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of [a data] breach."[lxv] Federal regulations define a breach as "the acquisition, access, use, or disclosure of [PHI]" in a way not permitted under federal regulations "that compromises the security or privacy" of the PHI.[lxvi] However, when a covered entity discovers that PHI has been impermissibly acquired, accessed, used or disclosed, it must presume that a data breach has occurred unless it conducts a risk assessment and determines that there is a low probability that the PHI has been compromised.[lxvii] To perform such a risk assessment, the covered entity, at a minimum, must consider the following four factors:

> (i) [t]he nature and extent of the [PHI] involved, including the types of identifiers and the likelihood of re-identification;
>
> (ii) [t]he unauthorized person who used the [PHI] or to whom the disclosure was made;
>
> (iii) [w]hether the [PHI] was actually acquired or viewed; and
>
> (iv) [t]he extent to which the risk to the [PHI] has been mitigated.[lxviii]

When a covered entity performs such a risk assessment, it must be sure to properly document and retain records demonstrating its compliance with the risk assessment requirements. HHS regulations place the burden on the covered entity to prove that (a) it provided all notifications required by HHS regulations, and/or (b) its risk assessment demonstrates that there is a low probability that PHI has been compromised.[lxix] Failure to create and maintain such documentation may result in significant penalties.

Once a covered entity discovers that it has suffered a data breach involving unsecured PHI, it must notify each individual whose PHI has potentially been compromised "without unreasonable delay" and at least within sixty (60) days after "discovery" of the breach.[lxx] HHS regulations define a covered entity's "discovery" of a breach as the earlier of the day on which the covered entity knew of the breach or when the covered entity would have known of the breach by "exercising reasonable diligence."[lxxi] In addition, HHS regulations consider a covered entity to have knowledge of a breach when the breach "is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity."[lxxii]

Further, HHS regulations require that notice of a breach to an affected individual must be written in plain language and must meet certain content requirements.[lxxiii] The breach notice must:

- describe the breach,
- provide the date of the breach,

- provide the date of discovery of the breach,
- provide the types of unsecured PHI that were potentially compromised in the breach,
- inform the individual(s) of steps that they may take to protect themselves from any potential damage resulting from the breach,
- describe the investigation of the breach and any steps taken to mitigate the harm to affected individuals and protect against further breaches,
- include contact procedures for any affected individuals who wish to ask the covered entity questions or learn additional information about the breach, including a toll-free telephone number, an e-mail address, a website or a postal address, and
- be sent by first-class mail to the last known address of the individual, or may be sent by e-mail if the individual has agreed to receive electronic notice.[lxxiv]

In addition to notifying affected individuals, a covered entity must notify the media in certain circumstances. For breaches involving the unsecured PHI of more than 500 residents of a state or jurisdiction, a covered entity must notify "prominent media outlets serving the State or jurisdiction."[lxxv] The notice of the breach to prominent media outlets must generally meet the same requirements as notice to individuals, in that it must be sent without unreasonable delay and within sixty (60) days of discovery of the breach.[lxxvi] In addition, the breach notice to media outlets must meet the same content requirements as notice sent to affected individuals.[lxxvii]

Additionally, a covered entity that suffers a data breach affecting the unsecured PHI of 500 or more individuals must notify the Secretary of HHS using the web portal available on the HHS's website.[lxxviii] Notification of the breach to the Secretary must be made contemporaneously with notification provided to affected individuals.[lxxix] However, for data breaches that involve the unsecured PHI of fewer than 500 individuals, a covered entity must maintain documentation of the breach and submit to the Secretary notification of the breach within sixty (60) days of the end of the calendar year in which the breach took place.[lxxx]

In a typical data breach involving the loss or theft of an unencrypted laptop containing ePHI, the health care provider will learn of the breach when a workforce member reports that his or her laptop has been lost or stolen. Through its incident response team, the health care provider should immediately investigate the incident to confirm that the laptop has in fact been lost or stolen, that it was not encrypted and that it contained unsecured PHI. After performing this initial investigation, the health care provider should engage counsel, report the theft to law enforcement and further investigate which individuals' PHI was present on the laptop.

Once the health care provider has identified all individuals whose PHI was potentially compromised, it should prepare to notify those individuals in compliance with HIPAA and the state law in each state in which an affected individual resides. If the breach is large enough to dictate that a call center be created for affected individuals, the health care provider should work with counsel and/or a public relations expert to prepare scripts and frequently asked questions.

Notification will then be sent to OCR, if required, and other regulatory agencies simultaneously with notification to individuals, unless state law provides otherwise. After notification is sent, the health care provider must respond to any requests for additional information from OCR or other regulatory agencies. Finally, the health care provider should return to normal operations and take any additional steps required to prevent future breaches. Following a breach involving a stolen laptop, a health care provider should be certain to immediately develop, implement and enforce policies and procedures requiring all workforce members to encrypt any laptops or other electronic media containing PHI.

V. Data Breach Notification Obligations of Health Care Providers under State Law

A. General Overview of Breach Notification Requirements under State Law

In forty-seven (47) states, the District of Columbia and United States territories, there are one or more statutes governing the notification obligations relating to data breaches involving personal information. Data breaches of health care providers often involve personal information that may fall under these statutes. Generally, these statutes provide that a person or entity that owns the personal information of another individual residing in that jurisdiction has a duty to notify individuals whose personal information has been compromised. While the person or entity owning the personal information may not reside in the same state as the affected individual, the person or entity owning the personal information must comply with the notification requirements in the state in which the affected individual resides. Thus, for breaches affecting more than a few individuals, the notifying person or entity will have to look to and comply with the state law in each state in which an affected individual resides. The notification obligations of a notifying person or entity may be complex in larger breaches, as laws in different states may differ with respect to the statutory definition of personal information, the definition of a data breach, the timing of notification, the individual(s) who must be notified, the content of the required notification and the method of notification.

For example, a common statutory definition of "personal information," such as the definition under Wisconsin law, includes an individual's last name and the individual's first name or first initial, in combination with the individual's Social Security number, driver's license or state identification number or financial account number, which includes credit or debit card numbers or any code or password that would allow access to the individual's financial account.[2][lxxxi] A common definition of a "breach" is the definition under Illinois law, which defines a breach as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information[.]"[lxxxii] However, most state statutes clarify that a breach does not include the authorized acquisition of data that has been de-identified, encrypted, redacted or made unreadable. Additionally, a good faith acquisition of personal information by an employee or agent authorized to acquire such information is generally not considered a breach.

Certain states have notification requirements beyond notifying the affected individual. A minority of states require that the state's Attorney General's Office or other regulatory agency be notified of the breach. Some states require notification to the Attorney General's Office for any breach involving an individual residing in that state, while other states require notification to the

[2] Wisconsin's definition of "personal information," unlike that of many other states, also includes an individual's last name and first name or first initial combined with the person's deoxyribonucleic acid (DNA) profile or biometric data.

Attorney General's Office only when the breach affects a larger number of residents of that state. Further, certain states require that breaches affecting a certain number of residents of that state must also be reported to the media and/or consumer reporting agencies.

B. Breach Notification Requirements under Michigan Law

Like the vast majority of states in the United States, Michigan has a data breach statute that requires notice to a Michigan resident when a health care provider discovers a data breach involving that resident's personal information.[lxxxiii] Michigan law defines "personal information" as a person's "first name or first initial and last name linked to [one] or more of the following data elements of a resident of this state: (i) [s]ocial security number[,] (ii) [d]river license number or state personal identification card number[,] [or] (iii) [d]emand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts."[lxxxiv] Thus, when a health care provider discovers that a data breach has resulted in a Michigan resident's unencrypted and unredacted personal information, as defined by the Michigan statute, having been accessed and acquired by an unauthorized person, the health care provider must give notice of the data breach to that resident.[lxxxv]

However, Michigan law allows a covered entity subject to HIPAA to comply with the Michigan data breach statute by complying with HIPAA regulations regarding notice of unauthorized access to customer information.[lxxxvi] Thus, if a health care provider subject to HIPAA regulations suffers a data breach that involves the unsecured PHI of Michigan residents, that health care provider must give notice to those Michigan residents as required by HIPAA. Assuming that the health care provider complies with all of its data breach notice obligations under HIPAA with respect to the affected Michigan residents, the health care provider does not need to comply with any additional notice requirements created under the Michigan data breach statute.[3] Importantly, however, a health care provider in Michigan may still have additional obligations to provide notice to individuals residing in other states, as not every state treats notification that complies with HIPAA regulations as sufficient to meet the obligations under that state's data breach statute.

VI. Best Practices for Health Care Providers in Responding to Data Breaches

A. Steps to Take Prior to Experiencing a Data Breach

Develop an Incident Response Plan

Health care providers should take proactive steps to prepare for a data breach to mitigate the costs and adverse effects associated with such incidents. As an initial step, health care providers should develop an incident response plan (IRP) and test the IRP, using tabletop exercises or mock data breaches, on a periodic basis. In addition, the provider should create roles for individual team members in responding to a data breach, known as an incident response team. Preparation prior to experiencing a data breach will allow the provider to quickly and appropriately take action when the almost inevitable breach occurs.

[3] In the unlikely event that a health care provider suffers a data breach that involves personal information as defined under Michigan law but does not involve unsecured PHI, as defined under HIPAA regulations, the provider should contact legal counsel to determine whether it must provide notice of the breach to Michigan residents under the Michigan data breach statute.

In addition, health care providers should develop procedures for reporting potential breaches to their incident response team, including 24-hour emergency contact information. Further, such procedures should be implemented for third parties with which the health care provider shares personal information or PHI, such as business associates or other vendors. Additionally, detailed procedures should be created for the key individuals on the incident response team, including procedures allowing them to determine the nature and scope of the incident, as well as the ongoing risks associated with the potential breach. Generally, the provider should focus on determining which records have been compromised, the information contained in those records and the identities of the individuals whose information has been compromised.

The incident response team, with the assistance of a forensics firm when appropriate, should also take appropriate steps to identify and isolate any affected systems to prevent the further unauthorized release of PHI. It is also critical that the team identify any other systems connected to the affected system(s) in order to minimize further damage. The team should further take steps to preserve needed data and evidence, including maintaining pertinent systems logs, activating auditing software, creating backup copies of altered files and recovering any lost data. In addition, the provider must document its actions to restore the integrity of its system(s) and any conversations it has with law enforcement relating to the breach.

Targeted Training and Preparation for Smaller and Mid-Size Providers

Smaller and mid-size health care providers with limited resources should focus on particular steps to minimize the risk of data breaches without incurring excessive prevention costs. Because small data breaches may cause health care providers to incur large costs in the form of CMPs, attorney's fees, negative publicity and other costs, even small providers must ensure that they have proper policies and procedures in place. All employees and workforce members should receive sufficient training on data privacy requirements and receive updates in training on a regular and periodic basis. Additionally, one of the easiest and most important steps small and mid-size health care providers can take is to ensure that all laptops and forms of electronic media containing PHI that are used by any of their workforce members are properly encrypted. Finally, providers should implement and regularly enforce policies that punish workforce members who fail to adhere to the provider's security guidelines.

Cyber Liability Coverage

Further, health care providers should consider purchasing cyber liability insurance to mitigate the financial harm resulting from a data breach. Numerous insurance companies offer policies that provide coverage relating to data breach costs. However, the available policies vary significantly with respect to how the health care provider should respond to data breaches, the costs and expenses covered and the premiums and deductibles of the policy. Health care providers should scrutinize the limitations that a cyber insurance policy might impose on their ability to respond to a data breach. Many policies require a health care provider to use specified forensics firms, law firms and/or public relations firms in responding to a data breach.

Moreover, cyber liability insurance policies may vary in the amounts covered for costs associated with (i) responding to a data breach, such as fees paid to forensics firms, law firms

and public relations firms, (ii) notifying affected individuals, and (iii) providing credit or identity theft monitoring to affected individuals. In addition, the cost of purchasing cyber liability insurance varies depending on the amount and types of coverage provided. Additionally, the premiums and/or deductibles of a cyber insurance policy may be affected by the size of the health care provider and the type and sophistication of its privacy and security controls. Larger health care providers are likely to have records containing PHI of more individuals and are thus are at greater risk of suffering very large costs associated with a data breach. As a result, a larger heath care provider will generally have to pay higher premiums and/or deductibles for a cyber insurance policy.

B. Steps to Take Once the Provider Has, or Suspects It Has, Suffered a Data Breach

Initial Investigation

Once a health care provider suspects that it may have suffered a data breach, it should immediately conduct an initial investigation to determine the nature and scope of the potential breach. Appropriate members of the incident response team should be engaged to identify the potentially compromised data. In addition, the incident response team must take all possible steps to contain the breach, which, depending on the circumstances, may include changing locks, access codes or passwords and notifying law enforcement. Further, the health care provider should limit the types of internal communications, particularly e-mail communications, that the incident response team uses to complete its initial investigation. Communications with third parties outside the incident response team, such as the media or workforce members not involved in the investigation, should be prohibited at this stage of the investigation.

As the investigation continues, the members of the incident response team who are engaged and actively involved in the investigation may change depending on the size and scope of the breach. When a breach is of a sufficient scope, the health care provider must obtain additional support, including outside counsel, forensic investigators, law enforcement and/or public relations experts. Engaging counsel earlier in a data breach investigation can help the health care provider to avoid pitfalls that may later be used against the provider, such as sending unnecessary, non-privileged e-mails relating to the potential breach that will be potentially discoverable in subsequent litigation. If the health care provider has obtained insurance coverage for data breaches, its procedures should provide for immediate notification to its insurance provider of a potential breach.

Generally, the health care provider should have an internal employee responsible for leading the incident response team under the guidance and direction of legal counsel. The incident response team should investigate the breach to determine all potential systems and/or data that may have been affected. The provider should take all appropriate steps, under the guidance of a forensics firm when necessary, to understand the cause of the potential breach, mitigate the harm to affected systems and prevent other systems/data from becoming compromised. In certain circumstances, the provider will need to notify appropriate law enforcement agencies early in the investigation stage to inform them of potential criminal activity and receive assistance in identifying the individuals responsible for the breach.

Breach Notification

After a health care provider has followed its protocols in identifying the breach and mitigating the resulting harm, the provider should begin the breach notification phase. The health care provider will generally need to engage counsel, if it has not done so already, to complete the required notifications, as most health care breaches require notice to individuals residing in numerous states and compliance with the law of each state. Depending on the size of the breach, the health care provider may also consider setting up a call center to provide information to affected individuals. Further, the provider should consider whether it will offer services such as credit monitoring or identity-theft protection services to affected individuals. In addition, the provider should prepare to respond to inquiries it will likely receive after providing notification of the breach, including inquiries from affected individuals, government agencies, employees, business associates and the media.

Assess Liability

With the assistance of legal counsel, the health care provider should assess the risk of civil litigation resulting from the breach. Further, the provider should determine whether any third parties have liability to the provider based on contractual indemnification provisions or through negligence in causing the breach. Depending on the cause of the breach, the provider may also need to assess whether responsible individual employees should be disciplined.

Post-Breach Review of Policies

After the health care provider has notified affected individuals, it will be able to return its data, systems and services to normal operational status. The provider should ensure that it documents the procedures used to respond to the breach and its efforts to provide proper notification of the breach. Additionally, health care providers should engage in a post-breach review to evaluate the procedures used and modify these procedures as needed. This post-breach review will help the health care provider to improve its privacy and data protection efforts, as well as allow it to update its privacy training programs.

C. Checklist of Steps in Responding to a Data Breach

When a health care provider suffers a data breach, it should use the below checklist to ensure it follows the appropriate steps in responding to the breach:

- Conduct an initial and immediate investigation of the nature and scope of the potential breach. The initial investigation should follow the procedures outlined in the IRP, including limitations on the team's communications regarding the breach.

- If the initial investigation determines that a breach may have occurred, engage all relevant members of the incident response team.

- Determine the media (computerized data or paper records) and the types of information (names, Social Security numbers or health information) that may have been affected.

- Identify the number of individuals potentially affected and where they reside.

- Conduct a preliminary internal assessment of the incident to determine whether a breach has, in fact, occurred.

- Assess the threat posed by the breach to determine which third parties need to be advised of the breach or retained by the health care provider, including business associates, vendors, legal counsel, cyber insurer(s), forensic investigators, law enforcement and public relations experts.

- Ensure that the entire team follows appropriate methods of communication for breach investigation, which may include limitations on e-mail communications and requirements that certain communications be conducted by telephone or in person.

- Take all necessary steps to contain the breach, including isolating any affected systems, identifying systems that are connected to affected systems, reconfiguring firewalls, updating antivirus software, changing passwords and modifying physical access controls.

- Take all necessary steps to preserve data and evidence and document all steps to restore the integrity of the affected system(s). Forensic investigators should be engaged to preserve compromised data.

- Conduct necessary interviews with key custodians of the data by counsel, human resources, information technology and/or forensic investigators. The investigation of the breach will evolve over time, with an emphasis on learning as much detail about the breach as possible, including the date, time and location of the breach, when the breach was discovered, the cause(s) of the breach and which data has been compromised.

- Assess all contractual and legal obligations that the health care provider may have as a result of the breach. The provider should also assess whether any third parties may have obligations to it as a result of the breach.

- Prepare a list of affected individuals and their current addresses. The provider must also determine whether OCR, state Attorneys General, other government agencies, consumer reporting agencies and the media must be notified.

- Prepare and coordinate notification to affected individuals and other required agencies or entities, including OCR, state Attorneys General, consumer reporting agencies and/or the media.

- Decide whether to create a call center for affected individuals, and if required, prepare escalation contacts, a list of frequently asked questions and answers and scripts for call center operators.

- Prepare to respond to inquiries regarding the breach from affected individuals, government agencies, business associates, employees, patients and the media. This preparation may include training employees to respond to such inquiries and/or creating a website regarding the breach.

- Inform all employees of the appropriate response to and/or where to direct inquiries from third parties regarding the breach.

- Determine whether to provide affected individuals with credit monitoring or identity theft protection services.

- Send all required notifications under HIPAA and state law. Outside counsel should review all notifications regarding the breach.

- Return all data and services impacted by the breach to normal operation.

- Document the health care provider's incident response and notification efforts.

- Conduct a post-notification internal review of the breach to make modifications to the provider's breach response policies and procedures.

- Update workforce training programs based on lessons learned from the breach.

D. Permanent Auditing of Health Care Providers by OCR

Historically, OCR has completed very few audits of health care providers and business associates to determine their compliance with HIPAA privacy practices. However, in September 2015, the HHS Office of Inspector General (OIG) issued a report entitled "OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards."[lxxxvii] In particular, the report's findings noted that OCR's pilot audit program had determined that fifty-four percent (54%) of covered entities failed to comply with at least one privacy standard.[lxxxviii] One of the main recommendations of OIG's report was that OCR implement a permanent audit program of covered entities and business associates to assess their compliance with privacy rules and regulations.[lxxxix]

As a result of OIG's report and recommendations, OCR submitted a memorandum to OIG stating that OCR would be implementing a permanent audit program.[xc] OCR expects to begin the second phase of its audit program in early 2016 by "updating [its] audit protocols, refining the pool of potential audit subjects, . . . implementing a screening tool to assess size, entity type and other information about potential audit subjects[, and] updating its electronic document management and investigations tracking system, called the Program Information Management System (PIMS)[.]"[xci] In light of OCR's intent to create a permanent audit program, health care providers should conduct a risk assessment that addresses privacy safeguards, protocols for data transmission security, encryption of devices and staff training on policies and procedures to comply with HIPAA privacy regulations.

E. Typical Questions from Enforcement Agencies after Reporting a Data Breach

Generally, upon learning of a data breach by a health care provider or other entity, HHS and other regulatory agencies will request the following information and/or documents:

- A detailed timeline of the incident, including when and how the entity discovered the breach and steps taken by the entity to mitigate the effects of the breach;
- A copy of any breach notifications and press releases issued by the entity that relate to the breach;
- Evidence of any actions to determine the root cause of the breach;
- A copy of the entity's Incident Response Plan;
- A copy of the entity's Written Information Security Plan;
- All policies and procedures relating to the physical, administrative and technical safeguarding of personally identifiable information and PHI;
- All policies and procedures relating to the entity's uses and disclosures of personally identifiable information and PHI;
- All policies and procedures relating to applying appropriate sanctions against workforce members who fail to comply with the entity's privacy policies and procedures;
- All documentation relating to any sanction that was applied against the workforce member responsible for the breach;
- A description of how various categories of customer or employee information are stored, including whether the information is encrypted and whether it is separated from other data;
- A description of how long information provided by customers, employees or patients is stored by the entity and whether any of this information is automatically deleted after a certain period of time;
- A description of the means, if any, by which customers can delete the information the entity stores about them;
- A copy of any security reports and/or forensic analyses, including any related correspondence and memoranda, concerning the incident; and
- An outline of any plan the entity has developed to prevent the recurrence of any such incident and a timeline for implementing that plan.

Health care providers that report a data breach should anticipate that regulatory agencies will ask the above questions and should ensure that they have prepared sufficient answers to these questions in advance of reporting a breach.

VII. Conclusion

Data breaches have increasingly become a part of doing business for health care providers. Small and mid-size health care providers should take the necessary preventive steps to protect themselves and to minimize the risk of and adverse effects from data breaches. While the risk of a data breach can never be eliminated entirely, creating and following proper policies and procedures can significantly reduce the ultimate harm that health care providers experience from a data breach when it inevitably occurs. For additional information on data breaches, notification requirements and best practices in responding to data breaches, health care providers should review the resources provided in end notes to this article.

[i] Caroline Humer and Jim Finkle, Reuters, *Your Medical Record Is Worth More to Hackers Than Your Credit Card* <http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924> (accessed January 29, 2016).
[ii] Resolution Agreement dated August 31, 2015, p 1 <http://www.hhs.gov/sites/default/files/cancercare-racap.pdf> (accessed January 26, 2016).
[iii] Resolution Agreement dated November 19, 2015, <http://www.hhs.gov/sites/default/files/lahey.pdf> (accessed January 26, 2016).
[iv] "Covered entities" are defined in HIPAA as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any PHI for which HHS has adopted standards. 45 CFR 160.103 [2015]
[v] Ponemon Institute LLC, *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* (May 2015).
[vi] *Id.* at p 10.
[vii] *Id.* at p 14.
[viii] *Id.*
[ix] Generally, a "business associate" is an entity that acts on behalf of or provides services to a covered entity that involve the potential use or disclosure of PHI. The definition of business associate can be found in 45 CFR 160.103.
[x] *See* 45 CFR 160.402, 160.404 (2015).
[xi] 45 CFR 160.304 (2015).
[xii] 45 CFR 160.306(b) (2015).
[xiii] *See* 45 CFR 160.402 (2015).
[xiv] 45 CFR 160.402(a) (2015).
[xv] 45 CFR 160.404 (2015).
[xvi] 45 CFR 160.408 (2015).
[xvii] 45 CFR 160.402(a) (2015).
[xviii] 45 CFR 160.404(b)(2)(i)(A) (2015).
[xix] 45 CFR 160.401, 160.402(b)(2)(ii)(A) (2015).
[xx] 45 CFR 160.410(c) (2015).
[xxi] *Id.*
[xxii] 45 CFR 160.401, 160.402(b)(2)(iii)(A) (2015).
[xxiii] 45 CFR 160.402(b)(2)(iv)(A) (2015).
[xxiv] 45 CFR 160.402(b)(2) (2015).
[xxv] Resolution Agreement dated August 31, 2015, p 1 <http://www.hhs.gov/sites/default/files/cancercare-racap.pdf> (accessed January 26, 2016); *see also* U.S. Department of Health & Human Services, *$750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies*, <http://www.hhs.gov/about/news/2015/09/02/750%2C000-dollar-hipaa-settlement-emphasizes-the-importance-of-risk-analysis-and-device-and-media-control-policies.html> (accessed January 26, 2015).
[xxvi] Resolution Agreement dated August 31, 2015, p 1 <http://www.hhs.gov/sites/default/files/cancercare-racap.pdf> (accessed January 26, 2016).
[xxvii] *Id.*
[xxviii] *Id.*
[xxix] *Id.* at pp 1–2.
[xxx] *Id.* at p 2.
[xxxi] *Id.* at pp 2, 5–10.
[xxxii] *Id.*
[xxxiii] *Id.*
[xxxiv] *Id.*
[xxxv] Resolution Agreement dated November 19, 2015, <http://www.hhs.gov/sites/default/files/lahey.pdf> (accessed January 26, 2016); *see also* U.S. Department of Health & Human Services, *HIPAA Settlement Reinforces Lessons for Users of Medical Devices*, <http://www.hhs.gov/about/news/2015/11/25/hipaa-settlement-reinforces-lessons-users-medical-devices.html> (accessed January 26, 2016).
[xxxvi] Resolution Agreement dated November 19, 2015, <http://www.hhs.gov/sites/default/files/lahey.pdf> (accessed January 26, 2016).
[xxxvii] *Id.*
[xxxviii] *Id.*
[xxxix] *Id.*
[xl] *Id.*
[xli] *Id.*
[xlii] Resolution Agreement dated April 21, 2014, <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf> (accessed January 26, 2016); *see also* U.S. Department of Health & Human Services, *Stolen Laptops Lead to Important HIPAA Settlements*, <http://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html> (accessed January 26, 2016).
[xliii] Resolution Agreement dated April 21, 2014, p 1 <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf> (accessed January 26, 2016).

[xliv] *Id.* at pp 2, 4–8.
[xlv] Resolution Agreement dated April 14, 2014, <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/ enforcement/ examples/qca_agreement.pdf> (accessed January 26, 2016); *see also* U.S. Department of Health & Human Services, *Stolen Laptops Lead to Important HIPAA Settlements*, <http://www.hhs.gov/about/news/2014/ 04/22/stolen-laptops-lead-to-important-hipaa-settlements.html> (accessed January 26, 2016).
[xlvi] Resolution Agreement dated April 14, 2014, pp 1–2 <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/ enforcement/ examples/qca_agreement.pdf> (accessed January 26, 2016).
[xlvii] *See* U.S. Department of Health & Human Services, *HHS Announces First HIPAA Breach Settlement Involving Less Than 500 Patients*, <http://www.hhs.gov/about/news/2013/01/03/hhs-announces-first-hipaa-breach-settlement-involving-less-than-500-patients.html> (accessed January 26, 2016).
[xlviii] Resolution Agreement dated December 28, 2012, <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/ examples/honi-agreement.pdf> (accessed January 26, 2016).
[xlix] *Id.*
[l] *See* U.S. Department of Health & Human Services, *HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records*, <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cornell/cornell-press-release/index.html> (accessed February 18, 2016).
[li] Resolution Agreement dated April 22, 2015, <http://www.hhs.gov/sites/default/files/cornell-cap.pdf> (accessed February 18, 2016).
[lii] *See Massachusetts v Beth Israel Deaconess Med Ctr, Inc*, unpublished Final Judgment by Consent of Defendant Beth Israel Deaconess Medical Center, Inc. of the Superior Court, entered November 20, 2014 (Docket No. 14-3627G).
[liii] Attorney General of Massachusetts, *Beth Israel Deaconess Medical Center to Pay $100,000 Over Data Breach Allegations*, <http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-11-21-beth-israel-data-breach.html> (accessed January 26, 2016).
[liv] *Id.*
[lv] *Id.*
[lvi] *See Massachusetts v Women & Infants Hosp of Rhode Island*, unpublished Final Judgment by Consent of Defendant Women & Infants Hospital of Rhode Island of the Superior Court, entered July 22, 2014 (Docket No. 14-2332G).
[lvii] Attorney General of Massachusetts, *Women & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations Involving Massachusetts Patients*, <http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-infants-hospital.html> (accessed January 26, 2016).
[lviii] *Id.*
[lix] *See In re Horizon Healthcare Servs, Inc Data Breach Litig*, unpublished opinion of the United States District Court for the District of New Jersey, 2015 U.S. Dist. LEXIS 41839, entered March 31, 2015 (Docket No. 13-7418); *Peters v St Joseph Serv Corp*, unpublished opinion of the United States District Court for the Southern District of Texas, 2015 U.S. Dist. LEXIS 16451, entered February 11, 2015 (Docket No. 4:14-CV-2872).
45 CFR 164.404(a)(1) (2015).
[lx] *See In re Horizon Healthcare Servs, Inc Data Breach Litig*, unpublished opinion of the United States District Court for the District of New Jersey, 2015 U.S. Dist. LEXIS 41839, entered March 31, 2015 (Docket No. 13-7418); *Peters v St Joseph Serv Corp*, unpublished opinion of the United States District Court for the Southern District of Texas, 2015 U.S. Dist. LEXIS 16451, entered February 11, 2015 (Docket No. 4:14-CV-2872).
[lxi] *Pisciotta v Old Nat'l Bancorp*, 499 F3d 629, 634 (7th Cir 2007); *Moyer v Michaels Stores, Inc*, unpublished opinion of the United States District Court for the Northern District of Illinois, 2014 U.S. Dist. LEXIS 96588, entered on July 14, 2014 (Docket No. 14-561).
[lxii] Allison Grande, Law360, *AvMed's $3M Pact Blazes New Path for Data Breach Plaintiffs*, <http://www.law360.com/articles/484008/avmed-s-3m-pact-blazes-new-path-for-data-breach-plaintiffs> (accessed January 28, 2016).
[lxiii] *Id.*
[lxiv] Michael Lipkin, Law360, *CORRECTED: Stanford, Contractors to Pay $4M To Settle Data Breach Action*, <http://www.law360.com/articles/520220/corrected-stanford-contractors-to-pay-4m-to-settle-data-breach-action> (accessed January 28, 2016).
[lxv] 45 CFR 164.404(a)(1) (2015).
[lxvi] 45 CFR 164.402 (2015).
[lxvii] *Id.* 164.402(2).
[lxviii] *Id.*
[lxix] *See* 45 CFR 164.414 (2015).
[lxx] 45 CFR 164.404(b) (2015).
[lxxi] *Id.* 164.404(a)(2).
[lxxii] *Id.*
[lxxiii] *Id.* 164.404(c).
[lxxiv] *Id.*
[lxxv] *Id.* 164.406(a).
[lxxvi] *Id.* 164.406(b).

[lxxvii] *Id.* 164.406(c).
[lxxviii] 45 CFR 164.408 (2015); *see also* U.S. Department of Health & Human Services, *Submitting Notice of a Breach to the Secretary*, <http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html> (accessed January 27, 2016).
[lxxix] 45 CFR 164.408(b) (2015).
[lxxx] 45 CFR 164.408(c) (2015).
[lxxxi] Wis. Stat. 134.98(1)(b) (2007).
[lxxxii] 830 ILCS 530/5 (2012).
[lxxxiii] *See* MCL 445.72.
[lxxxiv] MCL 445.63(r).
[lxxxv] *See* MCL 445.72(1)(a)(2).
[lxxxvi] MCL 445.72(10).
[lxxxvii] Department of Health and Human Services Office of Inspector General, *OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards*, <http://oig.hhs.gov/oei/reports/oei-09-10-00510.pdf> (accessed January 29, 2016).
[lxxxviii] *Id.* at p 7.
[lxxxix] *Id.* at p 11.
[xc] *Id.* at p 20.
[xci] *Id.* at p 21.