own *your audit*

HIPAA AUDIT PREPARATION

icemiller.com | @IceMillerLLP

IceMiller
LEGAL COUNSEL

table of contents

PART 1

Is your company subject to an OCR compliance audit?
In Phase 2, covered entities and business associates may be audited.

Key Points

Who is impacted?

- Covered entities: Health plans, health care clearing houses, and most health care providers.
- Business associates: Generally, anyone – typically, a vendor – handling protected health information on behalf of a covered entity.

What's at stake?

- Phase 2 audits are part of a larger program of ongoing compliance audits. The focus is expected to shift from education to enforcement.
- Non-compliance threatens individuals (patients and plan participants), as well as covered entities and their business associates.
- Privacy and security violations can subject individuals to financial and medical identity theft, as well as undermine their confidence in providers and plans.
- Violations also carry serious financial and reputational risks for covered entities and business associates.

Are you ready to own your audit?

Contact Ice Miller to get started on HIPAA Audit Preparation >

OCR's HIPAA Phase 2 Audits Are Here: Check Your Spam and Junk Folders

***Nicholas Merker,** Partner*

***Kimberly C. Metzger,** Partner*

***Christopher S. Sears,** Partner*

On March 21, the HHS Office for Civil Rights (OCR) announced its launch of the long-anticipated Phase 2 of the HIPAA Audit Program. OCR is currently collecting demographic information for a group of potential covered entity (CE) auditees, with the same for business associates (BAs) to follow.

All covered entities – including health care providers of all types and sizes, self-funded employer group health plans, and health care clearinghouses – as well as the full range of business associates, are eligible for audit. Receiving initial communications from OCR and providing demographic information does not mean OCR has selected your organization for audit. However, potential auditees must be on diligent lookout for the email, which includes checking appropriate spam and junk email folders on a daily basis, due to tight response deadlines. OCR will notify selected CEs auditees within the coming months, and begin the polling and selection process for BAs afterward. Desk audits of CEs and BAs are expected to conclude by the end of December 2016, and select, more rigorous and comprehensive site audits will then begin.

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires HHS to conduct periodic audits of CEs' and BAs' compliance with the Privacy, Security, and Breach Notification Rules. In 2011 and 2012, OCR conducted a pilot (Phase 1) audit of 115 covered entities, including a broad range of health care providers, health plans, and health care clearinghouses (OCR did not audit BAs). The pilot audit involved three steps: (1) developing audit protocols; (2) conducting an initial wave of 20 audits to test the protocols; and (3) conducting the full range of audits. Every pilot audit included a site visit and resulted in an audit report. HHS used the pilot audits primarily as a compliance improvement activity and to determine the most effective types of technical assistance and corrective action.

Phase 2 of the HIPAA Audit Program draws on OCR's evaluation of the pilot audits. Every covered entity and business associate – whatever its size and function – is eligible for audit. Sampling criteria for selection will include:

- Size of the entity;
- Affiliation with other healthcare organizations;
- Type of entity and its relationship to individuals;
- Whether an organization is public or private;
- Geographic factors; and
- Present enforcement activity with OCR.

OCR makes clear that it is "committed to transparency about the process," and will publish audit protocols "closer to conducting" the audits.

In Process: Selecting Auditees

OCR has begun obtaining and verifying CE contact information, and following up with requests for demographic information, to determine potential CEs auditee pools. OCR's initial communications will arrive by automated email and may be incorrectly identified as spam. CEs should check their junk and spam email folders daily for a communication from OCR. Note that savvy hackers may view this as an opportunity to conduct phishing campaigns. Entities who receive an email purportedly from OCR should verify that any attachments or links within the email are not malicious. Recipients will have only 14 days to respond as instructed in the communication and confirm identity and email contact information. Failure to respond will not shield a CE (or, later, a BA) from selection.

OCR is currently sending pre-screening questionnaires to potential CE auditees to gather data relevant to screening criteria. OCR will conduct a random sample of potential auditee pools and notify the CEs that have been selected for audits. OCR advises CEs to begin preparing lists of their BAs now, as CEs that are selected for audits will be asked to identify all of their BAs. OCR will use the CEs' inventories of their BAs to build its pool of potential BA auditees, and it will then notify the BAs that have been randomly selected for audits.

Upcoming: Notifying Auditees and Conducting Audits

In the "coming months," OCR will notify selected CEs and BAs, by email, of their upcoming audit. Phase 2 will include both desk and site audits. While audit protocols are designed to work with a broad range of CEs and BAs, their application may vary with the auditee's size and complexity. Audits will be limited to compliance with the HIPAA Rules, and will not address State-specific privacy and security laws. The first audits will be desk audits of CEs, followed by desk audits of BAs. The OCR's notification letter will introduce the audit team, provide more detail on the audit process, and describe "initial" document requests. Auditees will have 10 business days from the date of the request to submit requested documents and data electronically via a secure audit portal.

Auditors will examine the information submitted and provide the auditee with draft findings. Auditees will have 10 business days to review the draft findings and provide any written responses. Within 30 days of the auditee's response, OCR will prepare a final audit report and share it with the auditee.

While desk audits of CEs are in process, OCR will replicate the notification process for BAs. All desk audits will conclude by the end of December, 2016.

Next, OCR will schedule site audits that will examine a broader scope of HIPAA Rules requirements. Desk auditees may also be subject to a site audit. OCR will notify CEs and BAs of their selection for site audit, and will schedule an entrance conference to discuss the process and expectations. Site audits will last 3-5 days, and "will be more comprehensive and cover a wider range of requirements from the HIPAA Rules," according to OCR's announcement.

As with desk audits, auditees will have 10 business days to review and respond to draft findings, and OCR will issue a final report within 30 days of the auditee's response.

After the Audits

OCR will not post a listing of audited entities, or individual audit findings which clearly identify the audited entity. However, FOIA requests may require OCR to release audit notification letters and other audit information.

As with the pilot audits, OCR states that the Phase 2 audits "are primarily a compliance improvement activity." OCR will use aggregated audit results to better understand compliance efforts, and develop appropriate technical assistance, corrective action, and industry tools and guidance. However, OCR makes clear that a "serious compliance issue" may result in an investigation of the CE or BA.

What Can CEs and BAs do *Now*?

While OCR is sending its initial confirmatory emails, CEs and BAs should prepare for the possibility that they may be selected for an audit pool:

- Determine the person or persons at your organization OCR is most likely to identify as the "primary contact," and notify them to diligently monitor for the initial OCR communication. This should include daily checking of spam and junk email files.

- Consider an entity-wide communication informing of the potential for OCR communication, and the potential for phishing and malware attacks under guise of such communications. Instruct all workforce members to notify the Privacy Officer and/or Security Officer immediately (and tell them how to do it) if they receive a communication purporting to come from OCR – without clicking on attachments and links – so that attachments and links can be timely explored in a secure environment.

- Remember: CEs and BAs will have only 14 days to respond to the initial communication. If the OCR communication does not specify calendar v. business days, assume the shorter time period and respond accordingly. Failure to respond will not exempt your organization from audit.

- Covered entities: Identify your business associates, verify current contact information, and gather all business associate agreements.

- Identify an audit team who can respond immediately should your organization be identified as a preliminary auditee, and in the long-term should you be selected for audit.

- Gather documentation OCR is likely to request, including:
  - Privacy Rule (PR), Security Rule (SR), and Breach Notification Rule (BNR) policies and procedures.
  - Documentation of employee training (materials and participation).
  - Documentation of requests for access to PHI, and the organization's response.
  - Logs of unauthorized disclosures of PHI.
  - Results of SR risk analysis, and corrective action taken.
  - Documentation of the organization security management process.
  - Documentation of investigations of potential breaches of unsecured PHI, and breach notification.
  - Documentation of efforts to mitigate harmful effects of privacy breaches and security incidents.
  - Documentation of disciplinary procedures for workforce members that violate the HIPAA Rules.

- Review OCR's Phase 1 audit protocols to understand what upcoming protocols may look like.

- Contact counsel immediately should your organization receive an initial identification notice from OCR. Counsel can assist you in organizing documents and data OCR may request, filling any existing gaps (more on this below), and identifying any potential privilege issues – which should be asserted with extreme caution and mindfulness of potential consequences, if at all.

- Begin to fill potential compliance gaps now. While for purposes of the audit itself, OCR will likely consider only documentation existing at the time of the notification/request (and while, of course, your organization must be transparent about what existed when), you may have the opportunity to demonstrate best efforts by showing what you did after notification to identify and mitigate potential non-compliance.

OCR Releases Phase 2 Audit Protocol and Other Tools

***Kimberly C. Metzger,** Partner*

Without fanfare, OCR has released the protocol and several other tools for the recently-launched Phase 2 HIPAA compliance audits. The updated protocol identifies approximately 180 areas for potential audit inquiry: 89 from the Privacy Rule (addressing notice of privacy practices, rights to request privacy protection, access, administrative requirements, uses and disclosures, amendment, and accounting of disclosures), 72 from the Security Rule (administrative, physical, and technical safeguards), and 19 from the Breach Notification Rule. Areas of inquiry will vary among auditees: auditees will not necessarily be audited on every "key activity." The OCR's notification letter will inform the auditee of the areas of inquiry.

The new protocol builds upon and expands the Phase 1 protocol, and describes the areas of "audit inquiry" OCR will use to assess compliance with a particular "key activity" (HIPAA Rule standard or implementation specification) and associated "established performance criteria" (directives contained in the HIPAA Rules). OCR has issued general audit instructions along with the protocol:

1. References to "entity" in the protocol mean both CEs and BAs unless specifically identified as one or the other.

2. "Management" refers to the appropriate privacy, security, and breach notification official(s) or person(s) designated by the CE or BA to implement policies, procedures, and other standards.

3. The auditor will not necessarily request all policies and procedures for review.

4. Unless otherwise specified, all document requests are for versions in use as of date of the audit notification and document request.

5. Unless otherwise specified, selected entities should submit documents via OCR's secure online web portal in PDF, MS Word, or MS Excel formats.

6. If the requested number of implementation documents is not available, the entity must provide instances from previous years to complete the sample. If no documentation is available, the entity must provide a statement to that effect.

7. Workforce members include entity employees, contractors, students, and volunteers.

8. Information systems include hardware, software, information, data, applications, communications, and people.

For example: Many CEs and BAs are concerned about the state of their Security Rule risk analysis. The Security Rule requires covered entities and business associates to implement a *security management process* – "policies and procedures to prevent, detect, contain, and correct security violations."[1] Risk analysis is part of the security management process. The Security Rule defines "risk analysis" as "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 covered entity or business associate."[2]

- In standard HIPAA parlance, risk analysis is a *required implementation specification* for the security management process *standard*.
- In revised protocol language, risk analysis is a "required" "key activity" for the security management process, and the definition of *risk analysis* provides the "established performance criteria." To determine whether the audited CE or BA has met the established performance criteria (in other words, whether it has performed an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it holds), OCR will examine designated areas of "audit inquiry."

The revised protocol for risk analysis looks like this:

Audit Type	Section	Key Activity	Established Performance Criteria
Security **Required/ Addressable** Required	§164.308 (a)(1)(ii)(A)	Security Management Process -- Risk Analysis	§164.308(a)(1)(ii)(A): Conduct 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 covered entity or business associate.

Audit Inquiry

Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits?

Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?

Determine how the entity has implemented the requirements.

Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated.

Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted. Evaluate and determine whether the risk analysis or other documentation contains:

- A defined scope that identifies all of its systems that create, transmit, maintain, or transmit ePHI
- Details of identified threats and vulnerabilities
- Assessment of current security measures
- Impact and likelihood analysis
- Risk rating

Obtain and review documentation regarding the written risk analysis or other documentation that immediately preceded the current risk analysis or other record, if any. Evaluate and determine if the risk analysis has been reviewed and updated on a periodic basis, in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.

If there is no prior risk analysis or other record, obtain and review the two (2) most recent written updates to the risk analysis or other record, if any. If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an explanation as to the reason why.

Continuing with the risk analysis example, the revised protocol also describes areas of audit inquiry for the other three implementation specifications that, together with risk analysis, comprise the security management process standard: risk management,[3] sanctions policy,[4] and information system activity review.[5] If the CE or BA is selected for audit of its security management process, it should examine all four related key activity protocols (established criteria and areas of audit inquiry).

Of course, the security management process key activity protocols comprise but a small portion of the revised protocol. CEs and BAs selected for audit should work with counsel to determine, among other things, how to best use the revised protocol to prepare for their audit.

OCR is currently emailing potential audit pool members to confirm contact information, and has recently begun sending a prescreening questionnaire to these entities. The prescreening questionnaire consists of 30 questions, including general entity description questions (public or private? single- or multi-location? affiliation with/ownership by other entities?) and separate sections for Healthcare Providers, Health Plans, Healthcare Clearinghouses, and Business Associates.

CEs and BAs should review this questionnaire and begin gathering information that is not readily obtainable (e.g., number of patient visits in, and revenue for, the past fiscal year; number of claims processed monthly in the past fiscal year). While the prescreening questionnaire should not be time-consuming, the turnaround time will likely be short.

CEs and BAs should be alert for these OCR communications, and should ensure that individuals OCR might identify as the entity's "primary contact" check their junk and spam email folders daily (and be wary of potential phishing schemes). More information about the Phase 2 pre-audit process, and steps your organization can be taking now to prepare, can be found in *OCR's Phase 2 Audits Are Here: Check Your Spam and Junk Folders*.

OCR has also published a sample template for identifying business associates. This includes a sample spreadsheet for CEs to identify their BAs and contact information such as names, type of services provided, address, emails, and website URL. Regardless of whether a CE has received an initial OCR communication, working through this analysis privately is an excellent exercise to track BAs and keep their information current.

CEs and BAs should review the revised protocol and begin fill potential compliance gaps now. While for purposes of the audit itself, OCR will likely consider only documentation existing at the time of the notification/request (and while, of course, your organization must be transparent about what existed when), you may have the opportunity to demonstrate best efforts by showing what you did after notification to identify and mitigate potential non-compliance.

[1] 45 CFR 164.308(a)(1)(i)

[2] 45 CFR 164.308(a)(1)(ii)(A)

[3] 45 CFR 164.308(a)(1)(ii)(B)

[4] 45 CFR 164.308(a)(1)(ii)(C)

[5] 45 CFR 164.308(a)(1)(ii)(D)

HIPAA Covered Entities: Are Your Business Associates Ready for a Security Incident?

Kimberly C. Metzger, Partner

With OCR Phase 2 audits underway, many covered entities are taking a fresh look at their physical, technical, and administrative safeguards for electronic protected health information (ePHI). A comprehensive data security analysis, however, does not stop at the covered entity's own threshold. A covered entity must ensure the confidentiality, integrity, and availability of "all" ePHI the CE creates, receives, maintains, or transmits. (45 CFR 164.306(a)(1)). This obligation includes proper management of business associate relationships.

A business associate is a person or entity that performs certain activities or functions that require it to use or disclose PHI on the covered entity's behalf. Examples of BAs include third party administrators that assist plans with claims processing, and consultants that perform utilization review for hospitals. As the Security Rule makes clear, a CE may not permit a business associate to create, receive, maintain, or transmit ePHI on the CE's behalf unless the CE obtains "satisfactory assurances" that the BA will appropriately safeguard the information. (45 CFR 164.308(b)(1)). These satisfactory assurances are embodied in a written agreement ("business associate agreement" or BAA) that meets Privacy Rule requirements. This includes the BA's agreement that it will use appropriate safeguards to prevent uses and disclosures of PHI that violate the BAA. (45 CFR 164.314(a); 45 CFR 164.504(e)).

In a May 3, 2016 listserv mailing, OCR cautioned covered entities to consider how they will address a breach *by their business associate*. This is an area of insecurity for many CEs. While the Breach Notification Rule requires BAs to notify their CE after discovering a breach of unsecured protected health information,[1] OCR reports that a large percentage of CEs believe their BAs will not, in fact, notify them of breaches or security incidents.[2] OCR also reports that CEs find it "difficult" to manage security incidents involving BAs, and "impossible" to determine whether their BAs security policies and procedures are adequate to effectively respond to a breach.

According to OCR, covered entities should consider:

1. Defining in the Business Associate Agreement when and how the BA may use or disclose PHI, with any other uses, disclosures, breaches, or incidents to be reported to the covered entity. Potential incidents include:

- Attempts to gain unauthorized access to ePHI or a system containing ePHI
- Unwanted disruption or denial of service to systems containing ePHI
- Unauthorized use of a system that processes or stores ePHI
- Changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent

2. Indicating in the BAA the timeframe in which the BAA must report the breach or incident to the CE. Quick incident/breach reporting can:

- Ensure the CE can meet its obligation to timely report any breaches of unsecured ePHI to individuals, OCR, and (sometimes) the media
- Minimize damages associated with a breach
- Protect, and prevent further loss of, ePHI
- Preserve evidence for forensic analysis
- Regain access to, and secure, information systems

3. Identify in the BAA the type of information the BA must report to the CE. This should include (but is not limited to):

- BA name and contact information
- What happened, including dates of incident and discovery
- Types of unsecured ePHI involved
- What BA is doing to investigate, and protect against further incidents

4. Train workforce members on incident reporting.

5. Consider auditing and assessing the BA's security and privacy practices.

In its May 2016 report, *Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches,* the Brookings Institution highlighted several potential contributors to the increased number and severity of breaches and security incidents affecting health care data. Covered entities should consider whether and how these factors apply to them, *and to their business associates*:

- **Too many people have access to health care data.** The Brookings Institution reports that health care data are being shared more extensively, and in many cases, "most employees [at the "sharee"] have full access to patients' medical data." While the urgency inherent in medical care arguably favors broader access within health care providers, business associates – who do not provide direct patient care – can rely less on this argument.

To limit risk in this area, covered entities should ensure that their BAs comply with the Security Rule requirements for role-based access to ePHI: (1) Implement procedures for the authorization and/or supervision of workforce members who work with ePHI, or in locations where it might be accessed (45 CFR 164.308(a)(3)(ii)(A)); (2) implement procedures to determine that an employee's access to ePHI is appropriate (45 CFR 164.308(a)(3)(ii)(B)); and (3) implement procedures for terminating access to ePHI when employment terminates or roles change (45 CFR 164.308(a)(3)(ii)(C)).

- **Medical data are stored in large volumes and for a long time.** The Brookings Institution notes that "[t]he probability and consequences of a data breach are directly associated with the storage duration and volume of medical data." With a security incident or breach a virtual inevitability, CEs should be conscious of "minimum necessary" obligations affecting the BA relationship. CEs should make reasonable efforts to limit disclosures to BAs to the minimum PHI necessary to accomplish the purpose of the disclosure, and should in turn ensure their BAs request – and further disclose – only the minimum PHI necessary to accomplish *those* purposes. (45 CFR 164.314(a); 164.502(b)). A business associate agreement is not a license for a wholesale information dump. Attending to minimum necessary requirements will limit the amount of PHI at the BA to that which is actually necessary for the BA to do its job, and will leave less data exposed in the event of a security incident or breach.

CEs should likewise take care that their BAs do not retain ePHI longer than necessary to complete the contracted services. A compliant BAA should account for data at the end of the BA engagement, and should provide that the BA will: *"At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible*." (45 CFR 164.314(a); 164.504(e)(2)(ii)(J)). Limiting the duration of the BA's access to ePHI will also contain damages in the event of an incident or breach.

While business associates are now directly liable under the Security Rule and many aspects of the Privacy Rule, covered entities remain responsible for selecting their BAs, properly vetting their physical, technical, and administrative safeguards, and embodying the parties' agreement in a compliant BAA. OCR has provided suggestions on how CEs can help manage risks to ePHI held by business associates to a manageable level. Covered entities should be particularly mindful of their own, and their BAs', minimum necessary obligations to appropriately limit the amount of PHI that could be exposed by a breach at the BA. CEs should likewise make reasonable efforts to ensure role-based access to PHI at the BA, limiting the opportunity for human error.

[1] 45 CFR 164.410(a)(1)

[2] The HIPAA Rules define a "security incident" as an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations. (45 CFR 164.304). A "breach" generally means an impermissible acquisition, access, use, or disclosure that compromises the security or privacy of PHI. (45 CFR 164.402).

PART 2

How Can a Risk Assessment Protect Your Organization and Individuals?

Key Points

- Data breaches and security incidents are prevalent; almost certainly a matter of when, not if. A robust Security Rule compliance program helps you manage risks and vulnerabilities.
- A Risk Assessment is mandatory for covered entities and business associates and is the cornerstone of Security Rule compliance.
- The Security Rule provides flexibility for organizations to tailor the Risk Assessment to their unique circumstances.
- A risk management program built on Risk Assessment findings protects entities and individuals, and can mitigate damages in the event of a breach.

Are you ready to leverage a Risk Assessment for a strong compliance program?
Contact Ice Miller

Healthier Data, Healthier Patients: Cybersecurity and Better Health Outcomes

***Kimberly C. Metzger,** Partner*

Medical identity theft, and incomplete patient disclosure due to cybersecurity concerns, can be dangerous – even deadly – to individuals, and can compromise community wellness. Breaches of health information can have serious economic and other consequences for providers as well. The author of this article discusses the cybersecurity landscape in healthcare, medical identity theft, patient disclosures, and implementing a security management program for health information.

Breaches of health information can have serious consequences for both providers and patients. It is easy to imagine the financial implications of cybersecurity incidents and data breaches.[1] The effort and expense associated with investigation, forensics, mitigation of damages, lost good will and reputation, billing problems, and monitoring and untangling consumer credit are significant and can have far reaching effects for all parties.

While monetary losses are a large and well-known part of an incident or breach, compromised data security at health organizations can also contribute to a less recognized, but perhaps more insidious, problem: poorer health outcomes. Medical identity theft, and incomplete patient disclosure due to cybersecurity concerns, can be dangerous – even deadly – to individuals, and can compromise community wellness.

Health organizations hold a wide variety of highly confidential personally identifying information (“PII”) that can wreak havoc in the wrong hands. Names, addresses, dates of birth, Social Security and driver’s license numbers, and financial account information are data points wrongdoers traditionally seek to commit financial identity theft. Records from health organizations contain this information and more. By their very nature, health records include data of an extremely private and personal nature related to patients’ overall physical condition, disease states, medical ailments, disabilities, and insurance, including Medicare, Medicaid, and Social Security (“medical PII”). Breach and misuse of medical PII, or even the perceived risk of breach or misuse, can cause physical as well as financial harm. As Federal Trade Commission (“FTC”) Commissioner Terrell McSweeney remarked in March 2015:

1 A useful definition of “security incident” can be found in the HIPAA Security Rule: “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” (45 CFR 164.304.) A “breach” typically refers to an actual unauthorized acquisition, access, use, or disclosure that compromises the security or privacy of unsecured data.

- One of the most lucrative avenues for identity thieves has become the stealing and exploitation of medical records. Unlike other forms of identification, our medical records offer nearly complete portraits of our lives and data. These factors have made medical records, and more specifically children's medical records, the most valuable consumer information in the black market. Scammers can use the medical records of children to steal identities and commit frauds that have a good chance of remaining undetected until a child turns 18.[1]

Because health records contain information that could be particularly embarrassing if disclosed, a patient who is insecure about a provider's data practices might fear revealing sensitive, but highly relevant, medical information such as smoking status, risky sexual behavior, drug or alcohol use, and mental health concerns. If an incident or breach actually occurs, a patient's medical PII could be used to commit medical identity theft (the fraudulent use of medical credentials to receive or bill for healthcare), resulting in a "mixed medical record" and serious physical harm to the patient.

The Cybersecurity Landscape in Healthcare

Security incidents and data breaches are prevalent in health organizations. From cyberattacks and systems failures to employee negligence and malicious insiders, the question is really no longer if, but when and how, an incident or breach will occur. Small health care providers, who believe their size and low profile immunize them from attack, may actually be at higher risk because they are less likely to take protective action (and criminals know this).

The Ponemon Institute's recently-published Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data paints an unsettling picture: during the last two years, 65 percent of represented health care organizations experienced electronic-based security incidents, and 54 percent experienced paper-based security incidents. More than 90 percent had a data breach, and 40 percent had more than five breaches. The study estimates that the health care industry accounted for 44 percent of all 2013 data breaches – more than any other economic sector.

Several factors have converged to create a perfect storm on the healthcare landscape. First, electronic medical PII is more available than ever before. Both the American Recovery and Reinvestment Act and the Affordable Care Act incentivize – and sometimes require – healthcare providers to digitize patient data. Second, medical PII has high black market value. While estimates vary, one cybersecurity expert who monitored underground transactions posits that stolen health credentials can command 10-20 times the price of a U.S. credit card number.[2] Third, health organizations have lagged behind the more traditional targets (financial services and retail) in cybersecurity savvy. Because the transition to digitized health data is relatively recent, the healthcare sector has simply not been pushed earlier to prepare. In April 2014, the Federal Bureau of Investigation ("FBI") issued a private industry notification to healthcare providers warning "[t]he healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely. . . ."[3] Cybercriminals recognize that medical PII is a lucrative asset in a less secure environment.

Despite the "universal risk for data breach," the Ponemon study found that health organizations are not, overall, particularly confident of their ability to detect and respond to incidents and breaches:

- 58 percent report having policies and procedures in place to effectively prevent or quickly detect unauthorized access, loss, or theft of patient data.
- 53 percent report that personnel have the technical expertise to identify and resolve data breaches.
- Only 49 percent agree they have sufficient technologies to effectively prevent or quickly detect breaches.
- Only 33 percent report having sufficient resources to effectively prevent or quickly detect breaches.[4]

The study concludes:

Healthcare organizations . . . face a rapidly changing threat landscape. Cyber criminals recognize two

2 Remarks to the Identity Theft Resource Center, Washington D.C., March 18, 2015. 3 Caroline Humer and Jim Finkle, Your medical record is worth more to hackers than your credit card number. Reuters (September 24, 2014), accessed June 30, 2015 at http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924. 4 Jim Finkle, Exclusive*: FBI warns healthcare sector vulnerable to cyber attacks*. Reuters (April 23, 2014), accessed June 30, 2015 at http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbiexclusiv-idUSBREA3M1Q920140423.

critical facts of the healthcare industry: 1) healthcare organizations manage a treasure trove of financially lucrative personal information and 2) healthcare organizations do not have the resources, processes, and technologies to prevent and detect attacks and adequately protect patient data. While the findings reveal a slow but steady increase in technologies, the pace of investments is not fast enough to keep up with the threats to achieve a stronger security posture.[5]

Medical Identity Theft

Medical identity theft occurs when a wrongdoer uses health credentials to fraudulently bill for goods or services, or to obtain healthcare in someone else's name. The wrongdoer may accomplish this with the true patient's consent – for example, when the true patient shares health credentials with an uninsured family member or friend – or by stealing the true patient's medical PII. Medical identity theft is underappreciated, but on the rise. The Ponemon Institute estimates the number of victims increased from more than 1.5 million in 2012, to more than 1.8 million in 2013.[6]

Like its financial counterpart, medical identity theft can cause monetary loss, damaged credit, and reputational harm. Medical identity theft is unique, however, in its ability to cause physical injury via a "mixed medical record." When a person obtains medical care in another's name, the fraudulent user's medical information is integrated with the true patient's information in a single, corrupted medical record that does not accurately reflect the true patient's health condition. It is easy to imagine the potential for harm: The fraudulent user's blood type is given to the true patient, who has a different blood type. The fraudulent user's medication allergies are attributed to the true patient, who either receives a medicine to which she is allergic, or is denied a medicine to which she is not allergic. The fraudulent user's "no medications" history is attributed to the true patient, who is given a medicine that interacts with another that he is, in fact, taking.

These potential harms are more than theoretical. The 2013 Poneman survey queried 788 adults who reported they, or a close family member, were the victim of medical identity theft. Of those surveyed:

- 56 percent lost trust and confidence in their health care provider.
- 15 percent reported misdiagnosis because of inaccuracies in the health record.
- 14 percent experienced a delay in receiving medical treatment because of inaccuracies in the health record.
- 13 percent experienced mistreatment of illness because of inaccuracies in the health record.
- 11 percent were prescribed the wrong pharmaceutical.

Medical identity theft is clearly a quality of care issue.

Patient Disclosures

Healthcare providers' cybersecurity practices, and patients' perceptions of those practices, may have profound effects on both patients and public health. A 2014 study by researchers at the Harvard School of Public Health showed that patients who are concerned about their healthcare provider's cybersecurity practices are more likely to withhold medical information. According to this study, more than 12 percent of respondents had withheld information from their provider because of security concerns.[7] Federal government statistics indicate an even higher rate of withholding: compared to the overall population, individuals who strongly disagree that healthcare providers have reasonable protections in place for electronic health records are almost five times more likely to have withheld information from their provider (33 percent vs. seven percent).[8]

This withholding impacts both patient care and public health: Patients' withholding medical information from healthcare professionals may not only impact negatively on the patient directly, but could also potentially compromise the health of others and the quality of healthcare surveillance systems. The consequences to the individual may range from relatively minor ones (such as missed opportunities for tobacco cessation counseling or treatment because of non-disclosure of smoking status) to more serious medical consequences (such as potential compromise in the timeliness, quality, and appropriateness of medical care). Patients with infectious, notifiable conditions who withhold all or part of necessary medical information . . . may inadvertently put the lives of others at increased risk. Furthermore, non-disclosure, under information or misinformation may jeopardize the data quality of healthcare surveillance systems. This is of significant public health concern, since such surveillance systems depend on accurate data to monitor existing and emerging trends in health outcomes and provide the basis for policy and population-based interventions.[9]

5 Ponemon *Institute, Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* (the"Study"), p. 3. 6 *Id.* at 26. 7 Ponemon Institute, *2013 Survey on Medical Identity Theft*, p. 5. 8 Agaku et al. *Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers.* J. Am. Med. Inform. Assoc. 2014; 21:374-378, at 375. 9 The Office of the National Coordinator for Health Information Technology, *Health care providers' role in protecting EHRs: Implications for consumer support of EHRs, HIE and patient-provider communication.* ONC Data Brief: No. 15 (February 2014).

Most adults are, naturally, interested in their providers' health information practices. While the 2014 study has limitations, it indicates – and common sense dictates – that if a patient is concerned about the privacy and security of health records, he or she will be less likely to disclose sensitive health information. This, too, is a quality of care issue as well as a public health concern.

Healthier Data: Implementing A Security Management Program

Risk management is essential to every organization. While it is impossible to prevent every security incident and data breach, a security management program helps an organization build a culture of concern, determine potential exposure, and appropriately manage risk to an acceptable level. This, in turn, contributes to better individual and community health outcomes by building patient trust and maintaining the integrity health records. A robust program also helps health organizations meet applicable state and federal standards, including those found in the HIPAA Privacy and Security Rules, and the Medicare and Medicaid EHR Incentive ("Meaningful Use") Programs.[10] Finally, a strong data management program can help businesses successfully resolve consumer complaints, limit audits, enforcement actions, and penalties by the Department of Health and Human Services Office for Civil Rights ("OCR") (which enforces HIPAA) or the Federal Trade Commission (which enforces the prohibition against unfair and deceptive trade practices), and reduce liability under other applicable state and federal law.

Reasonableness is the cornerstone of both OCR's and FTC's approach to data security. For example, FTC states that a business's data security measures must be "reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[11] Many aspects of a program are therefore flexible, and scalable to the specific needs of an individual organization. However, successful security management programs share key components.

In its 2015 Guide to Privacy and Security of Electronic Health Information,[12] the Office of the National Coordinator for Health Information Technology ("ONC") provides a sample approach for implementing a security management process in healthcare. While this approach does not address all the requirements of Meaningful Use or the HIPAA Security Rule, it provides a basic framework for compliance:

- STEP 1: *Establish a culture of compliance, select a team, and build a knowledge base.* This will include designating a security officer, using qualified professionals to assist with a risk analysis, and promoting an organization-wide culture of protecting privacy and securing PII.
- STEP 2: *Document the organization's process, findings, and actions.* These records will serve as an accurate record for the workforce, and will prove essential if the organization is subject to a compliance audit.
- STEP 3: *Perform a Security Risk Analysis.* The risk analysis assesses potential threats and vulnerabilities to the confidentiality, integrity, and availability of electronic PII. In general, the risk analysis will involve determining where electronic PII exists and how it is created, received, maintained, and transmitted (creation of a "data map"); identifying potential threats and vulnerabilities to the data; and evaluating risks and their associated levels – how likely it is that threats will exploit existing vulnerabilities, and how this will impact the confidentiality, integrity, and availability of data. The results will inform the organization's risk management strategy.
- STEP 4: *Develop an action plan.* This involves mitigating the potential risks identified by the Security Risk Analysis, focusing on high priority threats and vulnerabilities. The action plan should account for the organization's characteristics and environment – and be feasible and affordable. The action plan should include administrative, physical, and technical safeguards, organizational standards, and policies and procedures.
- STEP 5: *Manage and mitigate risk.* This involves implementing the action plan, educating and training the workforce, communicating with patients, and updating vendor contracts.

9 Agaku et al. at 377. 10 Health organizations may also have to comply with other privacy and security laws and requirements, including those in or promulgated by 42 CFR Part 2 (confidentiality of alcohol and drug abuse records), the Family Educational Rights and Privacy Act (FERPA), Title X of the Public Health Service Act, the Genetic Information Nondiscrimination Act (GINA), private-sector contracts, state law, state boards of medicine, state associations, etc. 11 Prepared Statement of the Federal Trade Commission on *Data Breach on the Rise: Protecting Personal Information From Harm.* Before the Committee on Homeland Security and Governmental Affairs, United States Senate. Washington, D.C., April 2, 2014. 12 http://www.healthit.gov/providers-professionals/guide-privcy-and-security-electronic-health-information.

- STEP 6: *Monitor, audit, and update security on an ongoing basis.* This involves both monitoring the adequacy and effectiveness of the security infrastructure and making needed changes, and maintaining retrospective documentation – such as an "audit log" – of who, what, when, where, and how PII has been accessed.

ONC also offers its "Top 10 Tips for Cybersecurity in Health Care,"[13] generally applicable to organizations of all sizes:

1. ***Establish a security culture.***
    - Build a security-minded educational culture so good habits and practices become automatic.
    - Conduct information security education frequently, on an ongoing basis.
    - Ensure managers and other leaders set a good example in attitude and action.
    - Make taking responsibility for information security a core organizational value.
2. ***Protect mobile devices.***
    - Ensure mobile devices are equipped with strong authentication and access controls (ensure laptops have password protection, and enable password protection on mobile devices; take extra physical control precautions if password protection is not provided).
    - Protect wireless transmissions from intrusion.
    - Do not transmit unencrypted protected health information across public networks.
    - Encrypt data when it is necessary to commit health information to a mobile device, or remove a device from a secure area.
    - Do not use mobile devices that cannot support encryption.
    - Install and activate remote wiping and/or remote disabling.
    - Disable and do not install or use file sharing applications.
    - Install and enable security software, and keep it up-to-date.
    - Research mobile applications before downloading.
    - Maintain physical control: keep it with you or lock it in a secure location; lock the screen when not in use; do not let others use it.

13 http://www.healthit.gov/providers-professionals-newsroom/top-10-tips-cybersecurity-health-care.

3. ***Maintain good computer habits.***

   - Configuration management
     - Uninstall unessential software applications.
     - Use caution when accepting default or standard configurations when installing software.
     - Ask whether your electronic health record ("EHR") developer maintains an open connection to installed software to provide updates and support – if so, ensure a secure connection at the firewall and request that this access be disabled when not in use.
     - Disable remote file sharing and remote printing within the operating system.
   - Software maintenance
     - Automate software updates to occur regularly.
     - Monitor for critical and urgent patches and updates that require immediate attention, and act upon them as soon as possible.
   - Operating system maintenance
     - Disable user accounts for former employees quickly and appropriately. Close access to the accounts of involuntarily terminated employees before serving notice of termination.
     - Before disposal, sanitize computers and other devices that have had data stored on them. The National Institute of Standards and Technology ("NIST") publishes guidelines for disposal.
     - Archive old data files for storage if needed, or clean them off the system if not needed, subject to applicable data retention requirements.
     - Fully uninstall software that is no longer needed, including trial software and old versions of current software.
     - Work with your IT team or other resources to perform malware, vulnerability, configuration, and other security audits on a regular basis.

4. ***Use a firewall.***

   - Unless the EHR is completely disconnected from the Internet, install a firewall to protect against outside intrusions and threats.
   - Large practices that use a Local Area Network ("LAN") should consider a hardware firewall.

5. ***Install and maintain anti-virus software.***

   - Use an anti-virus product that provides continuously updated protection against malware, viruses, and other code that attacks computers through web downloads, CDs, email, and flash drives.
   - Keep anti-virus software up-to-date.

6. ***Plan for the unexpected.***

   - Create regular and reliable data backups.
   - Consider storing backup far from the main system.
   - Protect backup media with access controls.
   - Test backup media regularly for ability to properly restore data.
   - Have a sound recovery plan. Know what data was backed up, when backups were done, where backups are stored, and what equipment is needed to restore backups.
   - Keep the recovery plan securely and remotely, where an identified person has responsibility to produce it in an emergency.

7. ***Control access to health information.***

   - Configure electronic records to grant access only to people with a need to know.
   - Set access permissions using an access control list. Before setting permissions, identify which files should be accessible to which staff members.
   - Configure role-based access as needed. In role-based access, a staff member's role within the organization (for example: physician, nurse, billing specialist) determines what information he or she may access. Assign staff to the correct roles, and set access permissions for each role correctly, on a need-to-know basis.

8. ***Use strong passwords and change them regularly.***

   - Choose passwords that wrongdoers cannot easily guess. For example, a strong password may be of a certain length (the longer the better), combining upper- and lower-case letters, and special characters such as punctuation marks.
   - Do not include personal information in passwords, such as birthdates, one's own name or the names of family members or pets, Social Security numbers, or information on social networking sites or other locations that others could easily discover.
   - Require multi-factor authentication, such as passwords plus fingerprint scans or randomly-generated PINs. Configure systems so that passwords must be regularly changed.
   - Develop a password reset process to provide quick and easy assistance for forgotten passwords. This will discourage staff from writing down passwords.

9. ***Limit network access.***

   - Prohibit installation of software without prior approval.
   - Set any wireless router to operate only in encrypted mode.
   - Prohibit casual network access by visitors.
   - Ensure that file sharing, instant messaging, and other peer-to-peer applications have not been installed without explicit review and approval.

10. **Control physical access.**

    - Limit the opportunity for devices to be tampered with, lost, or stolen.
    - Document and enforce policies limiting physical access to devices and information.

Conclusion

The security of PII is a quality of care issue. Patient concerns can impact disclosure of important health information, and breach of medical PII can lead – among other things – to medical identity theft, a mixed medical record, and physical harm to the patient. While electronic health records offer many benefits to patient care, they also offer new and complex avenues for breach. Wrongdoers recognize both the value of health data, and its ever-increasing availability. They will exploit vulnerabilities to obtain this data, regardless of the organization's size or profile.

A robust security management program will guide organizations in identifying their own security holes and threat environment, and implementing a mitigation strategy to reduce potential harm to both the entity and its patients. Successful programs share key components, which may be mandated by applicable state or federal law, such as the HIPAA Security Rule. However, programs are also flexible, and scalable to the organization's size and complexity, the amount of PII it holds, and available resources.

Because patient perception may impact disclosure and, thereby, quality of care, organizations should proactively communicate with patients about cybersecurity. Communications should emphasize that the organization places a priority on the security and confidentiality of PII, including health information. These communications should be culturally appropriate, and take into account any particular needs of the patient population.

Most importantly, the organization should back these communications with documented, ongoing efforts to achieve and maintain a culture of commitment to the privacy and security of patient data. By achieving compliance, health organizations can protect both themselves and their patients, and improve the quality of individual care and community health.

A Skimpy Risk Analysis is Risky Business for HIPAA Covered Entities and Business Associates

***Kimberly C. Metzger,** Partner*

A privacy and security risk analysis is not only a regulatory requirement for covered entities and business associates, it is also good business. The author of this article explains the Security Rule risk analysis, which can inform decision-making at all levels of the organization, and protects both the organization and its patients by maximizing the confidentiality, integrity, and availability of electronic protected health information.

Covered entities and business associates will remember 2015 as "the year of the health care hack." The Department of Health and Human Services reports that 56 major hacks affected nearly 112 million individuals last year, including the record-breaking Anthem hack, which alone affected almost 80 million individuals. Strong incentives to digitize mean that electronic health data – including electronic protected health information (ePHI) – is more available than ever for criminal exploitation and accidental exposure. Although more electronic data is available, the health care sector is later to data security than commerce and finance, and therefore can be considerably less resilient when confronting privacy and security threats. Unfortunately, cybercrime is easier, with flourishing marketplaces for hacker skills and tools, forums to share successful social engineering tactics, and even distribution chains for faster monetization of health data. If digital data is a target for thieves, electronic health information is in the bullseye.

Background

Of course, criminals are not the only threat to the confidentiality, integrity, and availability of electronic health data. IT systems and processes may fail. Employees or third parties may not know how to protect ePHI, or may make mistakes when accessing, using, storing, or transmitting the data. A 2015 study by the Ponemon Institute reveals that employee negligence is the number-one data security concern of both covered entities and business associates surveyed.[1]

Given this threat environment, it is fair to say security incidents and data breaches are not a matter of "if," but "when." According to the Ponemon Institute:[2]

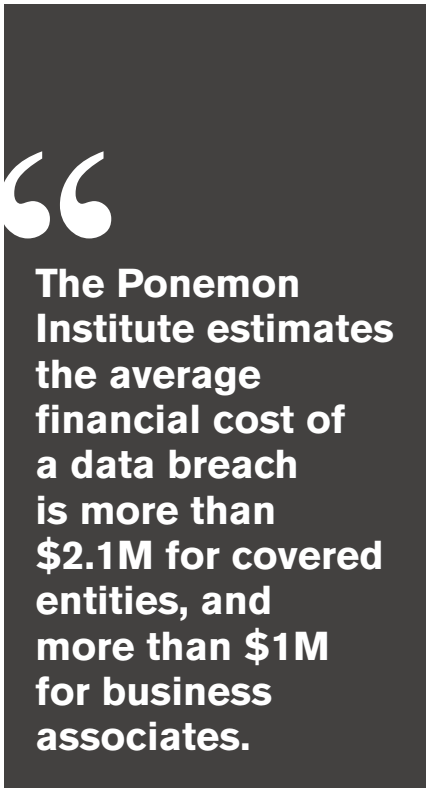
1 *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* (Ponemon Institute, May 2015). Ponemon surveyed 90 covered entities and 88 business associates. 2 *Id*.

- Ninety-one percent (91%) of covered entities, and 59% of business associates, had at least one data breach in the past two years. Forty percent (40%) of covered entities had more than five breaches, and 29% of business associates had more than two breaches.

- Criminal attack was the number-one cause of data breaches among covered entities, followed by lost or stolen devices, and employee negligence. However, employee negligence was the number-one cause of data breaches among business associates, followed by third-party negligence, and criminal attack.

- Sixty-five percent (65%) of covered entities, and 87% of business associates, had multiple security incidents involving the exposure, theft, or misuse of ePHI in the past two years. Fifty-eight percent (58%) of covered entities, and 70% of business associates, had 11-30 electronic-based security incidents.

- Lost or stolen devices were the number-one cause of security incidents for both covered entities and business associates, followed by spear phishing and web-borne malware attack.



The Cost of Data Breaches

Data breaches are expensive. The Ponemon Institute estimates the average financial cost of a data breach is more than $2.1M for covered entities, and more than $1M for business associates. Patients, too, may lose money to financial identity theft. However, breach costs are not limited to financial loss. Covered entities, business associates, and patients may suffer reputational injury as the result of a data breach. Patients may be subject to medical identity theft, and with it the potentially life-threatening consequences of a mixed medical record. Likewise, patients will likely refuse to disclose sensitive, yet vital, medical information – such as mental health concerns, HIV status, substance abuse, and the like – if they do not believe their doctors can keep this information safe and confidential. This, in turn, impacts public health reporting, making compromised data security in health care a true public health concern. The tentacles of harm reach far and wide.

Tools to Protect Against Privacy and Security Threats

The threat environment may be daunting, but the health care sector is far from helpless to protect itself and its patients. A variety of tools can assist covered entities and business associates in anticipating, protecting against, and responding to privacy and security threats, and preparing for the anticipated second round of OCR HIPAA compliance audits. One of the sharpest of these tools is the Security Rule risk analysis. A risk analysis is an

organization-wide "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability" of ePHI.[3] Risk analysis is a required implementation specification under the Security Rule, meaning that a CE or BA must perform the analysis in order to be compliant with the Security Rule. OCR Director Jocelyn Samuels has called comprehensive risk analysis, in combination with timely risk management practices, "the cornerstone of any good compliance program."

Recent High-Dollar Settlements

If you are not convinced that a comprehensive Security Rule risk analysis should be an integral part of your organization's electronic data management program, OCR's recent high-dollar settlements with covered entities should catch – and hold – your board's and C-suite's attention:

- University of Washington Medicine – December 14, 2015 ($750,000 resolution amount): Approximately 90,000 patients' ePHI was exposed when an employee downloaded an email attachment containing malware. UWM failed to follow its own policies in that it did not ensure affiliated entities conducted system-level risk assessments and properly identified risks and vulnerabilities. OCR Director Samuels said of the settlement: "All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise …. An effective risk analysis is one that is comprehensive in scope and is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data."

- Triple-S Management Corporation – November 30, 2015 ($3.5M RA): A former employee whose access rights were not terminated improperly accessed a database while working for a competitor, exposing more than 500 individuals' ePHI. Triple-S had not conducted a Security Rule risk analysis. Director Samuels emphasized the settlement was meant to convey an "important message" to covered entities about Security Rule compliance, including risk analysis.

- Lahey Hospital and Medical Center – November 25, 2015 ($850,000 RA): A laptop containing 599 individuals' unencrypted ePHI was stolen from an unlocked treatment room overnight. OCR found widespread non-compliance and determined, among other things, that Lahey had failed to conduct a Security Rule risk analysis. Director Samuels noted that workstations associated with medical devices often contain ePHI and are highly portable; therefore, "such ePHI must be considered during an entity's risk analysis, and entities must ensure that necessary safeguards that conform to HIPAA's standards are in place."

- Cancer Care Group, P.C. – September 2, 2015 ($750,000 RA): A laptop containing 55,000 patients' unencrypted ePHI was stolen from an employee's car. The entity had not conducted an enterprise-wide risk assessment addressing the "common practice" of removing hardware and media containing ePHI from the facility. Director Samuels emphasized: "Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information …. Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information."

- St. Elizabeth's Medical Center – July 10, 2015 ($218,200 RA): Employees' use of an internet file-sharing application to store documents resulted in the exposure of 595 individuals' ePHI. The entity had not analyzed the risks associated with using the application. Commenting on the enforcement, Director Samuels emphasized the importance of extending the risk analysis to internet-based applications.

- Anchorage Community Mental Health Services – December 2, 2014 ($150,000 RA): The hospital notified OCR of a breach involving 2,743 individuals after malware compromised the security of its IT resources. OCR determined that the incident was a direct result of the entity failing to identify and address basic risks, not regularly updating IT resources with available patches, and running outdated, unsupported software. Director Samuels stated: "Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis…."

[3] 45 CFR 164.308(a)(1)(ii)(A).

- New York Presbyterian Hospital/Columbia University Medical Center – May 7, 2014 (NYP = $3.3M RA; Columbia = $1.5M RA): The entities operated a shared data network, administered by both, that linked to NYP patient information systems. A physician employed by Columbia, who had developed applications for both entities, tried to deactivate a personal computer server on the network, resulting in ePHI being accessible on internet search engines. OCR found, among other things, that neither entity had conducted a risk analysis identifying all systems that accessed ePHI, and neither entity had an adequate risk management plan in place. OCR Acting Deputy Director Christina Heide emphasized that health care providers "need to make data security central to how they manage their information systems."

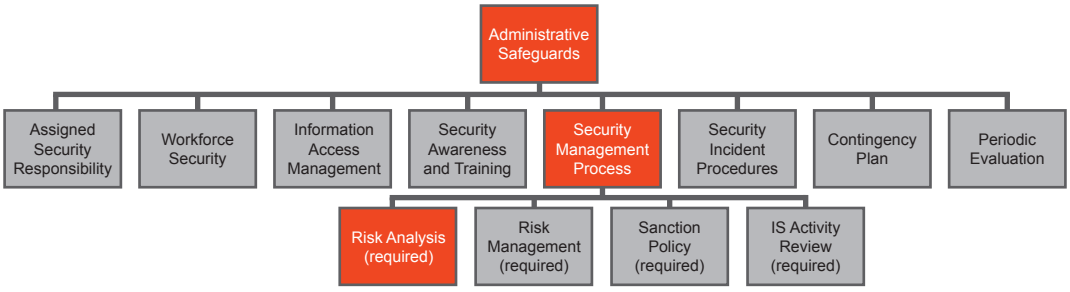
What exactly is a Security Rule risk analysis?

The Security Rule requires covered entities – and, now, business associates – to implement administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of ePHI. To be compliant with the administrative safeguards requirement, CEs and BAs must have in place a security management process, meaning the entity must implement "policies and procedures to prevent, detect, contain, and correct security violations."[4] The risk analysis is a required element of a CE's or BA's security management process, and requires the entity to perform an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability" of ePHI.[5]

Definitions

Some definitions are helpful to understanding the scope of a risk analysis, although not all of them come from the Security Rule:

- A "risk" is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Risks can arise from:
    - Unauthorized (malicious or accidental) disclosure, modification, or destruction of information;
    - Unintentional errors or omissions;
    - IT disruptions due to natural or man-made disasters; or
    - Failure to exercise due care and diligence in implementing and operating the IT system.[6]
- "Vulnerability" means a weakness in an information system, or a system's security procedures, internal controls, or implementation, that could be exploited by a threat.[7]



[4] 45 CFR 164.308(a)(1)(i). [5] 45 CFR 164.308(a)(1)(ii)(A). [6] NIST SP 800-30 r.1. [7] NIST SP 800-30 r.1.

- "Confidentiality" means data or information is not made available or disclosed to unauthorized persons or processes.[8]

- "Integrity" means data or information has not been altered or destroyed in an unauthorized manner.[9]

- "Availability" means data or information is accessible and useable upon demand by an authorized person.[10]

Factors to Consider

While the Security Rule requires a risk analysis, it does not mandate any particular form, format, or content and in fact is silent on these matters. This is because one size does not fit all covered entities and business associates. The Security Rule generally encourages a flexible approach to information security management (including the risk analysis), and a CE or BA may use "any security measures" that allow it to "reasonably and appropriately" implement Security Rule requirements. (45 CFR 164.306(b)). Factors to consider when evaluating what is reasonable and appropriate for your organization include:

- The entity's size, complexity, and capabilities.

- The entity's technical infrastructure, hardware, and software security capabilities.

- The cost of the contemplated security measures, and whether the entity will have to divert resources from other mission-critical functions to implement the measures.

- The probability and criticality of potential risks to ePHI – how likely is it that the identified threats will occur, and how serious will the consequences be if they do?

Conducting a Risk Analysis

While there is no "one right way" to conduct a risk analysis, critical steps include:[3]

1. *Prepare for the Risk Assessment:* Establish context for the task by defining the purpose and identifying the scope, assumptions, information sources, and analytic approaches to be used.

2. *Characterize the Organization's IT System*: Define the boundaries of the IT system, including the resources and information that comprise it. This includes, but is not limited to: Hardware; software; internal and external system interfaces; data and information; users and support personnel; system mission (what processes it performs); system and data criticality (value to the organization); and system and data sensitivity (level of protection required to maintain confidentiality, integrity, and availability).

3. *Gather Information:* Questionnaires; onsite interviews; review of relevant documents such as the organization's policies and procedures, system documentation, and security-related documentation.

4. *Identify Threat Sources:* What natural, human, and environmental sources threaten the confidentiality, integrity, and availability of ePHI? For adversarial human threat sources, assess capabilities, intentions, and targets. For non-adversarial human threat sources, look at the potential range of effects.

5. *Identify Threat Events:* What might happen, who or what might initiate it, and how relevant is it to the organization?

6. *Identify the Organization's Vulnerabilities and Predisposing Conditions:* Understand the nature and degree to which the organization, its mission, its business processes, and its IT systems are vulnerable to identified threat sources and threat events. What predisposing conditions within the organization increase or decrease the likelihood a threat event, once initiated by a threat source, will adversely impact operations, assets, or individuals?

7. *Determine Likelihood:* Will identified threat events actually result in adverse impacts to operations, assets, or individuals? Consider the characteristics of threat sources, identified vulnerabilities and predisposing conditions, and organizational susceptibility. What countermeasures or safeguards have been implemented, or are planned?

[8] 45 CFR 164.304. [9] Id. [10] Id. [11] 45 CFR 164.306(b). [12] See NIST Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments (September 2012).

8. *Determine Impact:* What effect will a threat event have on operations, assets, or individuals? Again, consider the characteristics of threat sources, identified vulnerabilities and predisposing conditions, and organizational susceptibility. What countermeasures or safeguards have been implemented, or are planned?

9. *Determine Risk:* What is the overall risk to the organization if a threat event occurs? Consider the resulting impact, as well as the likelihood that the event will actually occur.

Once the organization completes the risk analysis, it should communicate the results to decision-makers to support appropriate risk responses. The organization must also be dedicated to maintaining the risk analysis and keeping it current – monitoring policy and law; considering changes to the organization's structure, function, and mission; keeping abreast of the internal and external threat environment; assessing the effectiveness of risk responses; and verifying workforce training and compliance.

Conclusion

Risk analysis is not only a regulatory requirement for CEs and BAs, it is also good business. A robust risk analysis informs decision-making at all levels of the organization, and protects both the organization and its patients by maximizing the confidentiality, integrity, and availability of ePHI. Risk analysis is not a "once and done" checkmark, but rather an ongoing process throughout the organization's life cycle.

HIPAA gives CEs and BAs broad discretion to design and implement a risk analysis that best meets the organization's needs within its broader risk management program. The regulations afford flexibility in all aspects of the risk analysis, including formality, rigor, and level of detail; methodologies, tools, and techniques; format and content; and reporting. Cost, timeliness, and ease of use are also important considerations and will vary by organization. The only requirement is that the risk analysis be reasonable and appropriate under the circumstances.

Risk analysis may be mandatory for CEs and BAs, but it is foundational to any organization's risk management program. Any entity endeavoring to perform a risk analysis should consider not only what is reasonable and appropriate, but also (1) limitations inherent in the techniques, tools, and methodologies employed; (2) the quality and trustworthiness of data inputs; and (3) subjectivity in interpreting results. Armed with this knowledge, a CE or BA has the best chance of successfully framing, assessing, responding to, and monitoring risk to ePHI.

HIPAA Settlement Emphasizes Importance of Risk Analysis and Media Control Policies

***Kimberly C. Metzger,** Partner*

On September 2, 2015, the U.S. Department of Health & Human Services' Office for Civil Rights (OCR) – which enforces the HIPAA Privacy, Security, and Breach Notification Rules – announced that it reached a Resolution Agreement and Corrective Action Plan (RA/CAP) with the Cancer Care Group, P.C., to settle potential Security Rule violations. The covered entity will pay $750,000 and institute a "robust" corrective action plan.

Cancer Care Group, P.C., is a 13-member physician practice serving Indiana hospitals and clinics. In August 2012, the group notified OCR that a laptop containing unsecured protected health information (PHI) for approximately 55,000 patients had been stolen from an employee's car. The information included names, addresses, dates of birth, Social Security numbers, insurance information, and clinical information.

The OCR's investigation revealed the covered entity had been in "widespread non-compliance" with the Security Rule since before the breach. The group had not performed an enterprise-wide risk analysis, and did not have a written policy in place to address the "common practice" of removing hardware and electronic media containing PHI from the facility. According to OCR, a risk analysis could have identified removal of unencrypted backup media as an area of significant risk to the organization, and a written policy could have directed employees as to their responsibilities under these circumstances. Under the terms of the CAP, Cancer Care will conduct a risk analysis; develop and implement a risk management plan; review and revise policies and procedures; and review and revise its training program.

The Cancer Care RA/CAP emphasizes the importance of a robust, thorough, entity-wide risk assessment for ePHI. According to OCR Director Jocelyn Samuels:
"Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information …. Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information."

The HIPAA Security Rule requires covered entities and business associates to conduct an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information" they hold. (45 CFR 164.308(a)(1)(ii)(A)). Small health care providers are not exempt from this requirement. While entities are not required to outsource their risk assessment, the services of an experienced professional will assist in providing a RA that will withstand an OCR

compliance review. The regulations do not specify a particular form of risk assessment, and there are many approaches to take. However, the risk assessment must begin with a thorough data map that identifies all locations and flows of ePHI – including portable electronic devices and copiers that store data. Most importantly, the risk assessment is not a "once and done" process. The entity must review, correct, modify, and update its RA to account for changes in the law as well as in the entity's environment and ePHI locations and flows.

There is no better time for covered entities and business associates to evaluate their risk assessment and ensure they are in compliance. As OCR Director Jocelyn Samuels emphasized during her keynote address at a September 2, 2015 HIPAA security conference in Washington, D.C., the upcoming second round of OCR compliance audits will focus on key compliance areas such comprehensive and timely risk assessment.[1] Director Samuels noted she hopes the audit process will "send a message that complying with HIPAA is serious business." *Id*.

The Cancer Care RA/CAP also emphasizes the importance of security for laptops and other portable electronic devices. The federal government's Office of the National Coordinator for Health Information Technology (ONC) offers health care providers and other organizations suggestions for managing mobile devices used by health care providers and professionals:

- **Decide** whether mobile devices will be used to access, receive, transmit, or store ePHI or used as part of the organization's internal networks or systems (for example, the EHR system).
- **Assess** how mobile devices affect the risks (threats and vulnerabilities) to the organization's ePHI.
- **Identify** the organization's mobile device risk management strategy, including privacy and security safeguards.
- **Develop, document, and implement** the organization's mobile device policies and procedures to safeguard PHI.
- **Train** providers and professionals on best practices for mobile device privacy and security.

ONC also offers its Top 10 Tips for Cybersecurity in Health Care, which emphasize mobile device security.

The Security Rule risk assessment is a cornerstone of compliance and is mandatory for covered entities and business associates of all sizes. The Cancer Care RA/CAP emphasizes the importance of both risk assessment and portable mobile device security. Attending to the ONC's guidance, and engaging an experienced professional, can assist covered entities and business associates in meeting their compliance goals. This, in turn, will safeguard patient data, lessen the likelihood of a breach, and enable the entity to perform well in the event of an OCR compliance audit.

[1] Marianne Kolbasuk McGee, *New HIPAA Compliance Audit Details Revealed*, http://www.govinfosecurity.com/hipaa-compliance-audits-on-way-a-8518 (accessed September 3, 2015).

PART 3

Ongoing Training | Protect Your Business

Key Points

- A compliance program is only as strong as the people behind it.
- Workforce training is mandatory and helps you protect data and minimize risk.
- Ongoing data privacy and security training keeps your workforce up-to-date and will help satisfy auditors.

Do you need workforce training to protect your business?
Contact Ice Miller >

A Well-Trained Workforce Can Mitigate Risks and Vulnerabilities

Deepali Doddi, Associate

Kimberly C. Metzger, Partner

With the recent media emphasis on external threat sources such as phishing, ransomware, and other web-borne malware, it is easy to forget that many, if not most, data breaches and security incidents are rooted in simple human negligence – or ignorance. Whether it's clicking a bad link, failing to secure a laptop, or misdirecting a fax or email, unintended acts can have enormous consequences for individuals, covered entities, and business associates alike. In a 2015 survey by the Ponemon Institute, health care organizations listed "employee negligence" as their most troubling security threat, and a full 95% of organizations surveyed had experienced a security incident involving a lost or stolen device. Patient privacy can suffer, as well, if well-meaning but uninformed workforce members impermissibly use or disclosure protected health information (PHI), do not allow individuals to adequately exercise their rights under the Privacy Rule, or do not provide individuals with timely notifications of breaches, as required by the Breach Notification Rule.

While it is impossible to eliminate all risks to PHI and each of the organization's vulnerabilities, a well-trained workforce goes a long way toward helping CEs and BAs manage risks and vulnerabilities to an acceptable level. The Privacy Rule, Security Rule, and Breach Notification Rule each contain standards and implementation specifications related to workforce training:

1. Privacy Rule: "A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by [the Privacy Rule], as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity." The CE must provide this training within a "reasonable time" of onboarding, and must re-train within a "reasonable time" of a material change to policies or procedures that affect a workforce member's functions. The CE must document this training as the Privacy Rule requires.

2.Security Rule: "A covered entity or business associate must …. [i]mplement a security awareness and training program for all members of its workforce (including management)." This includes implementing (a) periodic security updates; (b) policies and procedures for guarding against, detecting, and reporting malicious software; (c) procedures for monitoring log-in attempts and reporting discrepancies; and (d) procedures for creating, changing, and safeguarding passwords.

3. Breach Notification Rule: The Breach Notification Rule incorporates many of the Privacy Rule's administrative requirements by reference, including those regarding workforce training. A covered entity, therefore, must train workforce members on its policies and procedures related to complying with the Breach Notification Rule and document workforce members' receipt of such training.

[1] Ponemon Institute, 2015. Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data [2] 45 CFR 164.530(b)(1) [3]45 CFR 164.530(b)(2)(i)(B), (C). [4]45 CFR 164.530(b)(2)(ii) and 164.530(j)(1). Note that a covered entity must maintain documentation of the training for a minimum of six years. See 45 CFR 164.530(j)(2). [5]45 CFR 164.308(a)(5)(i). [6]45 CFR 164.308(a)(5)(ii). [7]45 CFR 164.414(a).

While the Privacy, Security, and Breach Notification Rules tell CEs and BAs what they must do (i.e., train), they do not tell regulated entities how to do it. Rather, the HIPAA Rules are flexible and scalable to accommodate CEs and BAs of all types and sizes. Like almost every aspect of the HIPAA Rules, there is no "one size fits all" way to comply. However, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) offers suggestions for compliance with the Security Rule training requirement that translate effectively to the Privacy Rule and Breach Notification Rule, as well:

STEP 1: Conduct a Training Needs Assessment

(A) Determine your organization's training needs, and

(B) Interview and involve key personnel in assessing needs.

Ask yourself:

• What awareness, training, and education programs are needed? Which are required?

• What are our current efforts in this space, and how well are they working?

• What gaps exist, and what more do we need to do?

• How will we prioritize content and audience?

STEP 2: Develop and Approve a Training Strategy and Plan

(A) Address the specific Privacy Rule, Security Rule, and Breach Notification Rule policies and procedures that require awareness and training; and

(B) Outline your program's scope, goals, target audience, learning objectives, deployment methods, evaluation and measurement techniques, and frequency.

Ask yourself:

• What procedure will we implement to track training, and ensure that everyone who needs training receives it?

• What training is needed to address specific topics based on job responsibility?

• When should training be scheduled?

• How will we ensure that non-employees (trainees, contractors, interns) are trained?

STEP 3: Security Rule: Protection for Malicious Software, Log-in Monitoring, and Password Management

(A) As reasonable and appropriate, train workforce members on procedures for (1) guarding against, detecting, and reporting malicious software; and (2) monitoring log-in attempts and reporting discrepancies; and (3) creating, changing, and safeguarding passwords; and

(B) Incorporate information about roles and responsibilities into training and awareness methods.

Ask yourself:

• Do workforce members understand the importance of timely application of system patches to protect against malware and exploitation of vulnerabilities?

• Are workforce members aware that log-in attempts may be monitored?

• Do workforce members that monitor log-in attempts know to whom to report discrepancies?

• Do workforce members understand their roles and responsibilities in selecting a password of appropriate strength, changing their password as required, and safeguarding their password?

STEP 4: Develop Appropriate Awareness and Training Content, Materials, and Methods

(A) Select topics for inclusion in training materials;

(B) As reasonable and appropriate, incorporate new information from trusted outside sources (e.g., online IT security websites; email news alerts); and

(C) As reasonable and appropriate, use a variety of media and avenues based on workforce size, location, job responsibilities, etc.

Ask yourself:

• Do workforce members have access to your Privacy Rule, Security Rule, and Breach Notification Rule policies and procedures?

• Do workforce members know whom to contact, and

how to handle, a privacy or security incident?

• Do workforce members understand the consequences of noncompliance with your policies and procedures?

• Do workforce members who travel with PHI know how to handle portable media physical security, and other information security?

• Have you researched available training resources? Who will deliver the training?

• What is your training budget?

STEP 5: Implement Training

(A) Schedule and conduct training outlined in your strategy and plan;

(B) Implement reasonable techniques to disseminate privacy and security messages throughout the organization: newsletters, screen savers, videos, email blasts, staff meetings, and computer-based training;

Ask yourself:

• Have all workforce members received adequate training to fulfill their job functions?

• Are sanctions consistently applied for failure to complete required training?

STEP 6: Implement Reminders: Provide periodic privacy, security, and breach notification updates and reminders to workforce members and business associates.

Ask yourself:

• What methods are available, or already in use, to make or keep workforce members and business associates aware of privacy and security (e.g., posters, booklets)?

• Do you perform all-workforce refresher training at least annually?

• Do you train all new hires within a reasonable time of onboarding, and refrain from allowing them to access PHI until trained?

• Do you reinforce privacy and security topics during staff meetings?

STEP 7: Monitor and Evaluate Training Plan

(A) Keep your privacy, security, and breach notification training programs current;

(B) Re-train on material changes to policies and procedures, as well as the organization's threat and vulnerability environment;

(C) Monitor training program implementation to ensure all employees participate; and

(D) Implement corrective action when problems arise.

Ask yourself:

• Do you monitor and document workforce training and professional development programs?

• How are new workforce members trained?

• How are new business associates trained?

Thoroughly training your workforce on your HIPAA policies and procedures is necessary to not only satisfy regulatory requirements, but also reduce the occurrence of security incidents, breaches, and consumer complaints. Investing in a robust and meaningful HIPAA training program will go a long way to ensuring that your organization creates a culture of compliance.

PART 4

ICE MILLER'S MOCK AUDIT PROGRAM | TEST YOUR PREPAREDNESS

Key Points

- OCR has launched Phase 2 of its formal HIPAA Audit Program, and will soon audit 100-200 covered entities and business associates for compliance with the HIPAA Privacy, Security, and Breach Notification Rules.
- With the increasing rigor of HIPAA audits and fines, now is the right to invest in your HIPAA compliance program.
- Resolving any gaps in your HIPAA compliance program will reduce the likelihood of breaches and consumer complaints, and help you avoid protracted government investigations and any associated penalties.
- Ice Miller's Audit Preparation Program will pair a team of experienced health data privacy and security attorneys with your organization for a mock desk and on-site audits.

Are you ready to fill the security gaps to protect your business?
Contact Ice Miller >

Ice Miller Data Security and Privacy: OCR Audit Preparation

***Deepali Doddi,** Associate*

***Kimberly C. Metzger,** Partner*

***Nicholas Merker,** Partner*

Ice Miller is pleased to announce that Deepali Doddi has joined the firm's Data Security & Privacy Practice Group. Deepali is a five-year veteran of HIPAA audits stemming from her time as a senior investigator with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). She was lead investigator in the North Memorial Health Care case, which resulted in a monetary settlement of $1.55 million for alleged noncompliance with the HIPAA Rules.

The experience and bench strength Deepali brings to our practice comes at the right time. OCR has launched Phase 2 of its formal HIPAA Audit Program, and will soon audit 100-200 covered entities and business associates for compliance with the HIPAA Privacy, Security, and Breach Notification Rules. With the increasing rigor of HIPAA audits and fines, now is the right time to invest in your HIPAA compliance program. Ice Miller's Audit Preparation Program will pair a team of experienced health data privacy and security attorneys with your organization for a mock desk audit focusing on:

- Evaluating your privacy and security policies and procedures against HIPAA Rules standards;
- Determining whether you have conducted an organization-wide Security Rule risk assessment evaluating potential risks and vulnerabilities, and a plan to manage risks to an appropriate level;
- Assessing your incident response plan and breach notification procedures;
- Reviewing your notice of privacy practices and HIPAA patient authorization forms;
- Identifying your business associates (including subcontractor business associates), and reviewing whether you have entered into compliant business associate agreements with them;
- Examining your processes for handling patient requests for access, amendment, accounting of disclosures, and confidential communications; and
- Reviewing whether your organization maintains documentation specifically required by the HIPAA Rules.

We also offer mock on-site audits, including interviewing workforce members, evaluating administrative, physical, and technical safeguards, and collecting relevant documents. Once the mock audit process is complete, we will prepare a comprehensive written report of findings, and provide concrete recommendations for improving HIPAA Rule compliance. We will meet with your HIPAA compliance team to discuss our findings and recommendations, and help you formulate the best going-forward plan.

Even if OCR does not select your organization for a Phase 2 audit, solidifying your HIPAA compliance measures now will protect your patients or plan participants, and leave you well-positioned to respond to an audit inquiry during a later stage of OCR's permanent audit program. Resolving any gaps in your HIPAA compliance program will reduce the likelihood of breaches and consumer complaints, and help you avoid protracted government investigations and any associated penalties.

Ice Miller's Data Security and Privacy team is available to assist you in bolstering your HIPAA compliance program. If you are interested in learning more about Ice Miller's OCR Audit Preparation Program, please contact Kim Metzger (CIPP/US, CIPM), Nick Merker (CISSP, CIPT), or Deepali Doddi (CIPP/US).

Key Contacts

Nicholas R. Merker
Partner
312-726-2504
nicholas.merker@icemiller.com

Kimberly C. Metzger
Partner
317-236-2296
kimberly.metzger@icemiller.com

Stephen E. Reynolds
Partner
317-236-2391
stephen.reynolds@icemiller.com

Christopher S. Sears
Partner
317-236-5891
christopher.sears@icemiller.com

Taryn E. Stone
Partner
317-236-5872
taryn.stone@icemiller.com

Eric McKeown
Of Counsel
317-236-2124
eric.mckeown@icemiller.com

Deepali Doddi
Associate
312-726-7134
deepali.doddi@icemiller.com

@IceMillerLLP

IceMiller
LEGAL COUNSEL

own your audit

HIPAA AUDIT PREPARATION

icemiller.com | @IceMillerLLP