Black Market PHI Does Exist: Why It's Time to Take Security Risk Assessments Seriously

By Katherine Downing, MA, RHIA, CHPS, PMP

Many health information management (HIM) experts have wondered whether there is protected health information (PHI) on the black market. In short, the answer is "yes." According to a 2012 Ponemon Institute study, 90 percent of healthcare organizations surveyed have had at least one data breach in the past two years.[1] It is possible that some of this breached data is funneling into the black market. Implementing a risk analysis process can examine potential threats and vulnerabilities discovered during a risk assessment and prioritize those risks based on the probability and potential effect on the organization and patient. Risks may be mitigated, transferred, researched, or accepted depending on what option is most reasonable for the organization.

Of the organizations surveyed in the Ponemon study, the average number of data breaches over the past two years was four. The average number of lost or stolen records per breach was 2,769. The types of patient data most often involved in breaches was lost or stolen medical files, billing, and insurance records. And the top three causes for a data breach were lost or stolen computing devices, employee mistakes, and third-party errors, according to the Ponemon study, begging the question—where is this stolen PHI ending up? In some cases it is put up for sale.

Medical Identity Theft Feeds the Black Market

An estimated 1.84 million people were victims of medical identity theft in 2013, according to the Ponemon Institute, which expects that number to rise. In addition they estimate that about 36 percent of victims in 2012 incurred out-of-pocket expenses including reimbursement for services provided to imposters, legal fees, and identity protection services. The average cost for these victims amounted to $18,660, and in a few cases exceeded $100,000.[2] According to examples collected by the World Privacy Forum, a research group that seeks to educate consumers about privacy risks, the uses for stolen PHI have included the following:

- One identity thief in Missouri used the information of actual people to create false driver's licenses. The thief used one of the false licenses to enter a regional health center, obtain the health records of the woman she was impersonating, and leave with a prescription in the stolen name.
- A Pennsylvania man found that an imposter had used his identity at five different hospitals in order to receive more than $100,000 in treatment. The integrity of the medical record became a big issue for HIM professionals at those facilities.[3]

It is not just individual identifiers such as name, date of birth, address, insurance plan numbers, and Social Security numbers that consumers now need to protect. The stakes have become higher. On the black market a full packet of individual identifiers plus information gathered on social networking sites such as Facebook and LinkedIn can be worth $1,500 per individual. On Facebook, thieves can gather an individual's mother's maiden name, their spouse's name, and other family information. On the social media site LinkedIn, thieves can access information including a full work history, including dates for each previous position and locations where the individual has lived.

"They're hitting us and hitting us hard," says Timothy Menke, head of investigations for the Office of Inspector General at the Department of Health and Human Services, in an interview with CNN. "Organized crime involvement in healthcare fraud is widespread."[4] So how exactly is this data getting to organized crime syndicates? Identity thieves are one part of the equation, but consumers and patients play a role, too.

Figure 1. Nine Risk Analysis Process Steps to Follow

1. System Characterization:

   - Create an inventory of applications and systems
   - Group assets: Applications and support systems (workstations, laptops, network, etc.)

2. Threat Identification

   - Identify reasonably anticipated threats
   - Consider: Acts of nature, acts of man, and/or environmental threats

3. Control Assessment

   - Assess: What controls are in place?

4. Vulnerability Identification

   - Assess: What controls are missing?
   - Identify how applications or systems could be exploited

5. Likelihood Determination

   - Decide: What is the probability of each threat occurring?

6. Impact Analysis

   - Rate possible impacts as: High, Medium, Low
   - Evaluate: What would the risk identified do to my organization?

7. Risk Determination

   - Calculate a risk score

8. Recommended Controls

   - Provide recommendations to reduce or manage risks appropriately

9. Results Documentation

   - Create a summary of key findings, recommendations, and estimates to implement
   - Document management's decisions: Mitigate, transfer, or accept risk

Source: Susan Lucci and Tom Walsh Consulting, LLC

Lessons Learned from the Financial Industry

Exposure to healthcare breaches may seem like a new problem, but it's one similar to what the financial industry has been dealing with for many years. Lessons learned from the banking industry can help prevent and fix healthcare breaches as well. According to information posted on the website Identity Theft Blog in 2008, the banking industry accounted for 93 percent of a total 285 million compromised records. The following conclusions can be drawn from the lessons of that industry:

- Most data breaches resulted from a combination of events rather than a single action
- In 69 percent of the cases the breach was discovered by a third party
- Nearly all of the records compromised in 2008 were from online assets
- Eastern Europe is notorious for having organized cybercrime outfits that play a major role in breaches[6]

While sale of PHI on the black market is a concern in healthcare, some would argue the industry's main concern is patient safety and quality of care. When someone uses PHI for the purpose of illegally obtaining healthcare services, medical devices, insurance reimbursement, or prescription drugs, this does present a risk to the integrity of the medical record, patient safety, and quality of care. The reason for this risk in integrity is that the patients' information is now intermingled with that of the imposter, resulting in risk to patient safety based on clinical information such as blood type, medical conditions, and allergies.

Employ Risk Management to Combat Theft

With the recent boom in electronic health records (EHRs), more and more healthcare data is being stored electronically. Security risk management and assessment steps must be taken to protect our electronic assets. Managing risk is an essential step in operating any business, and it is impossible to eliminate all threats. However, healthcare organizations typically conduct a periodic risk analysis to determine their potential exposure. A risk analysis allows organizations to develop strategies to manage those risks appropriately.[7]

The concept of risk management is not new to healthcare, but conducting a risk analysis for information technology can be challenging. The HIPAA Security Rule and the "meaningful use" EHR Incentive Program require covered entities to perform a risk analysis. An assessment must address the following HIPAA Security Rule standard:

- **§164.308(a)(8),** Evaluation, which states that organizations must "Perform a periodic technical and nontechnical evaluation, based initially upon the standards and implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

The HIPAA Security Rule requires covered entities and business associates as well as their agents and subcontractors to conduct a risk analysis and implement measures "to sufficiently reduce those risks and vulnerabilities to a reasonable and appropriate level." Specifically, the rule requires compliance with the following:

- **164.308(a)(1)(ii)(A),** Risk analysis, which requires organizations to "…conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information…"
- **§164.308(a)(1)(ii)(B),** Risk management, which requires organizations to "…implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level…"[8]

The HIPAA Security Rule applies to a variety of organizations ranging from large healthcare systems to small physician practices—as well as their business associates. Thus the standards for how an organization must approach a risk analysis are flexible. An organization must base its decision on several factors, including:

- The organization's size, complexity, and capabilities
- The organization's technical infrastructure, hardware, and software security capabilities
- The costs of security measures
- The probability and criticality of potential risks to electronic protected health information (ePHI)

A risk analysis determines how to meet the HIPAA Security Rule's implementation specifications and whether an alternative security measure appropriately meets the intent of an implementation specification. However, the rule's preamble states "Cost is not meant to free covered entities from this [adequate security measures] responsibility." If the cost is reasonable—and a security measure or control would reduce risk significantly—then an organization of any size should consider implementing the control, especially if the risks are high or moderate.

In addition, healthcare organizations striving to meet the meaningful use criteria must conduct a risk analysis. Stage 1 meaningful use criteria includes the following measure: "Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process."

Stage 2 meaningful use criteria specifically says, "Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP’s [eligible provider’s] risk management process.”[9]

AHIMA’s Practice Brief “Security Risk Analysis” reviews the regulatory requirements of an effective security risk analysis and provides an overview of how to conduct a risk analysis. Figure 1 above illustrates the nine risk analysis process steps as detailed in this Practice Brief.

Notes

1. Ponemon Institute. “Third Annual Benchmark Study on Patient Privacy & Data Security.” December 2012. http://lpa.idexpertscorp.com/acton/attachment/6200/f-0033/1/-/-/-/-/file.pdf.
2. Ponemon Institute. “Third Annual Survey on Medical Identity Theft.” June 2012. http://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf.
3. Ollove, Michael. “Identity Theft Isn’t Just About Credit Cards—It’s About Health.” *Denver Post*. February 8, 2014. http://www.denverpost.com/nationworld/ci_25094885/identity-theft-isnt-just-about-credit-cards-mdash.
4. Chernoff, Allan, and Sheila Steffen. “Organized Crime’s New Target: Medicare.” CNN.com. October 24, 2009. http://www.cnn.com/2009/CRIME/10/22/medicare.organized.crime/.
5. Clearwater Compliance. “HIPAA Security Risk Analysis Tips—What Some CEOs Don’t Understand About HIPAA.” April 2, 2013. http://abouthipaa.com/hipaa-compliance-guides/hipaa-security-risk-analysis-tips-what-some-ceos-dont-understand-about-phi/.
6. Douglas, Rob. “Rise in Data Breaches, Organized Crime Involved.” Identity Theft Blog. April 15, 2009. www.identitytheftblog.info/identity-theft/data-breach-organized-crime/1366/.
7. AHIMA. “Security Risk Analysis and Management: An Overview (Updated).” *Journal of AHIMA* 84, no. 11 (November–December 2013): expanded web version.
8. US Department of Health and Human Services Office for Civil Rights. “HIPAA Administrative Simplification—45 CFR Parts 160, 162, and 164.”
9. Office of the National Coordinator for Health IT. “Meaningful Use Regulations.” http://healthit.hhs.gov/portal/server.pt?open=512&objID=2996&mode=2.

Katherine Downing (kathy.downing@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
. "Black Market PHI Does Exist: Why It’s Time to Take Security Risk Assessments Seriously" *Journal of AHIMA* 85, no.5 (May 2014): 50-53.