HCCA®
HEALTH CARE
COMPLIANCE
ASSOCIATION

Compliance TODAY

October 2013

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Why compliance matters to the enforcement community

Loretta Lynch
U.S. Attorney, Eastern
District of New York

See page 16

27
Medicaid vs. Medicare claims audit appeals: A road less clear
Cornelia M. Dorfschmid and Lisa Shuman

35
Sunshine Act reporting: Minimizing consulting and royalty payment risks
Stephanie J. Kravetz

41
OIG issues updated guidance on exclusion: What it means for providers
Lester J. Perling

47
Be part of the solution: Stop medical identity fraud
Marita Janiga

by Adam H. Greene

Finding your Snowden: Identifying insider threats by employees and contractors

» Identify and mitigate risks of contractor employees causing data breaches.
» Limit types of information that is made available to employees and contractors.
» Regularly review system activity for suspicious patterns.
» Consider technology like data loss prevention to limit sensitive information leaving systems.
» Prepare for responding to a breach caused by an employee or contractor.

***Adam H. Greene** (adamgreene@dwt.com) is a Partner in the Washington DC offices of Davis Wright Tremaine LLP and Co-Chair of its Health Information Practice Group.*

Greene

In June 2013, media shocked the world with stories of top secret intelligence programs of the National Security Agency (NSA).[1] Edward Snowden, a former employee of an NSA contractor, soon took credit for the leaks in a saga that, as of the writing of this article, continues to captivate the public. This article is not intended to treat Edward Snowden's actions positively or negatively overall—the ethics of what Snowden did are the subject of a great deal of debate. But what all sides seemingly can agree upon is that Snowden's actions represent a significant data breach for the NSA.

Although Snowden's riveting tale of espionage and asylum may seem far removed from the world of healthcare, it offers a number of important lessons to healthcare providers and health plans.

Limit access to sensitive information

One of the questions that arose after Snowden revealed himself is how this single employee had access to so much sensitive NSA information. It is unlikely that Snowden had authorized access to all of the documents that he revealed, but he probably was aided in gaining access by his status as a contractor employee.

Healthcare organizations need to carefully consider who within and outside of their organization has access to sensitive information. For example, which employees and contractor employees have access to Social Security numbers or sensitive clinical information?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) requires a covered healthcare provider or health plan to: (1) identify which persons need access to protected health information (PHI); and (2) reasonably limit their access to the categories of PHI that are needed.[2] The HIPAA Security Standards for Protection of Protected Health Information (Security Rule) then applies these "minimum necessary" requirements to electronic information, requiring covered entities to implement policies and procedures for managing access to information, including addressing the granting of access, termination of access, ensuring that the level of access is appropriate, and putting in place technical controls to prevent unauthorized access.[3]

Organizations can use the Snowden incident as an impetus to reexamine whether they have appropriately limited access to PHI among employees and contractors. For example, who actually needs access to Social Security numbers to perform their job responsibilities? Is access to a full Social Security number necessary, or can the organization mask all but the last four digits? Also, which employees need access to sensitive clinical information?

It is unlikely that granting access too liberally will lead to international incidents, but it may lead to excessive employee snooping and use of PHI for identity theft.

Regularly review system activity

A review of Snowden's access to sensitive documents likely would have revealed that he was collecting information for unauthorized purposes. In the wake of the Snowden leak, the NSA is purportedly considering new technologies to review system activity and identify potential leakers.[4]

Healthcare organizations need not attempt to implement NSA-level pattern recognition technology, but the Security Rule does require covered entities to implement mechanisms to record and examine activity in information systems that contain PHI.[5] Such mechanisms can take many forms. Healthcare providers and health plans can conduct manual reviews. They can implement centralized auditing software that employs algorithms to identify patterns of potential inappropriate access. Most likely, organizations may need to perform some combination of technological and manual review.

Some things, such as an employee snooping on a single record, can be very difficult to catch. But employees or contractors who are serially abusing their authorized access are a different story. Organizations should ask themselves, if an employee is viewing a large number of Social Security numbers or patient records, what mechanisms are in place to ensure this raises a flag? Covered entities should pay particular attention to what systems may contain Social Security numbers or financial account numbers but are not readily subject to monitoring (e.g., older legacy systems). Organizations may need to limit access to such systems, document the limits on monitoring them, and consider whether an upgrade is feasible.

There will always be sophisticated persons, such as Snowden, who know the system well enough to avoid raising alarms. But there also will be plenty of less sophisticated employees and contractors who will be caught through reasonable information system monitoring.

Man the exits

Even if Snowden appropriately had access to some of the sensitive information he leaked, at some point he took it out of the system. It may have been expected that, in the course of his duties, he would need to download or print sensitive documents. On the other hand, it may have been another opportunity to catch him. The NSA has indicated that it is instituting a new “two-man rule” to place checks on downloads of sensitive information by even the highest level system administrators in the wake of the Snowden incident.[6]

Healthcare providers and health plans, as part of their risk management and information system activity review, should consider technology such as data loss prevention (DLP) to identify and potentially prevent sensitive information from leaving the network. Such technology potentially can thwart minor leaks (e.g., a clinician sending a patient file to his or her personal e-mail account because of convenience) and major disasters (e.g., an employee downloading a spreadsheet with thousands of Social Security numbers onto a USB drive to provide to an identity theft ring).

Recognize the risks of contractor employees

The NSA found itself the center of an international storm, not because of the acts of an employee, but rather because of a contractor's employee. The NSA cannot operate alone, but rather relies on a large number of contractors.

Healthcare organizations are no different. Healthcare providers and health plans rely on a large number of contractors in order to function. The U.S. Department of Health and Human Services (HHS) website provides information about large health care breaches (those affecting 500 or more individuals). Between September 2009 and May 2013, the HHS website lists 627 large breaches affected over 22 million individuals.[7] Of these breaches, 138 (22%) are attributable to the act of a business associate rather than a covered entity. Furthermore, these business associate breaches tended to be disproportionately larger than those of covered entities, affecting 12.5 million individuals (56%).

Accordingly, healthcare providers and health plans can institute all the safeguards in the world, but if they do not have a handle on the activities of their contractors, a large breach may be inevitable. Before providing the equivalent of top secret information to a contractor, the healthcare organization may want to consider what it knows about that contractor's employees and information security. For example, does the contractor conduct background checks of employees who will have access to sensitive information? If the contractor will be maintaining a large volume of sensitive information, has the contractor had its information security independently audited? And, if the contractor has a breach, who will pay the resulting costs, such as breach notification, credit monitoring, and defense of any resulting lawsuits?

Unfortunately, with limited resources, healthcare organizations often are not in a position to reasonably scrutinize the practices of all of their contractors. Additionally, contractors may understandably limit what information they release about their information security practices in order to avoid providing third parties a roadmap to their security. Healthcare organizations may wish to categorize their contractors based on risk, focusing their attention on those with the most sensitive information and those with the least-known information security systems.

Think like a spy

The reports of the NSA and Snowden incident read like a Hollywood movie script rather than the sort of issues that healthcare organizations are likely to encounter, but compliance officers and others within healthcare organizations may consider using a little espionage themselves. Instead of simply waiting for information security problems to surface, providers can consider taking more active steps to root out potential breaches of information security.

For example, healthcare providers or plans can deploy "honeypots" to attract employees or contractors who abuse their access. The National Institute of Standards and Technology describes honeypots as "hosts that have no authorized users other than the honeypot administrators because they serve no business function; all activity directed at them is considered suspicious."[8] In layman's terms, a honeypot is a fake file or system that is attractive to unauthorized persons.

Healthcare providers and health plans can create fake files, such as "patient Social Security numbers" and see if the files are accessed. Such access may help identify an employee or contractor who seeks to compromise information for identity theft or other purposes. Keep in mind, an employee accessing a honeypot alone is not clear evidence that the employee seeks to compromise PHI. Organizations should consult with counsel if considering such security measures.

Even the best will fail

A final lesson of the Snowden incident is that even one of the most sophisticated security agencies in the world can suffer a significant data breach. Where does that leave the rest of us?

No matter how many safeguards a healthcare organization puts in place, there will always be opportunities for employees or contractors to bypass them. Often, the best that healthcare providers and health plans can do is to put in place reasonable safeguards. Although perfect security may be unattainable, using the lessons from incidents like the NSA's can help organizations improve their safeguards and reduce information breaches caused by employees and contractors.

Finally, no matter how mature an organization's information security program, it should be prepared for the day that it discovers its Snowden. This means putting in place a strong incident response plan and practicing it.

1. *See, e.g.*, Glen Greenwald: "NSA collecting phone records of millions of Verizon customers daily." *The Guardian*, June 5, 2013. Available at http://bit.ly/1aonSSo
2. 45 C.F.R. § 164.514(d)(2)(i).
3. 45 C.F.R. §§ 164.308(a)(3)(ii) and (4)(i) and 164.312(a)(1).
4. Audie Cornish: "Defense Department Trying To Plug Leaks Before They Happen." National Public Radio, June 14, 2013. Available at http://n.pr/19Fp6YE
5. 45 C.F.R. § 164.312(b).
6. Chloe Albanesius: "NSA Implements 'Two-Man Rule' to Prevent Future Leaks." *PC Magazine*, July 19, 2013. Available at http://bit.ly/18SF2nY
7. Department of Health and Human Services: Breaches Affecting 500 or More Individuals. Available at http://1.usa.gov/15ON3cQ
8. Karen Scarfone, Peter Mell: *Guide to Intrusion Detection and Prevention Systems, Special Publication 800-94 Revision 1 (Draft).* National Institute of Standards and Technology, July 2012. Available at http://1.usa.gov/1aAD3vf