Protecting Patient Privacy in the Cloud

K Royal, JD, CIPP/E, CIPP/US

Urgent message: *The shift in medical practice from written charts to integrated digital platforms has dramatically increased the visibility, size, and magnitude of health-care information breaches. There are specific steps urgent care operators should take with vendors to protect patient information in this new technological environment.*

The news makes it seem that data breaches occur on a fairly regular basis. The Ponemon Institute even named 2014 as the year of megabreaches.[1] An online chart created by David McCandless of Information Is Beautiful shows the world's biggest data breaches; it can be filtered by industry and the method of data leak.[2] Personal data are valuable, and medical data have very rich information indeed.

Some of the more recent breaches lately have affected the health-care field and are not limited to patient data. For example, in February 2015, Anthem Inc. announced a breach of more than 80 million records. More recently, in June 2015, Medical Informatics Engineering (MIE), an electronic health record vendor, announced a cyberattack of more than 4 million individuals. MIE is not the first business associate, as defined under the Health Insurance Portability and Accountability Act (HIPAA), to report a breach.

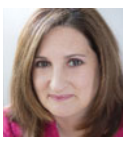
On the breach report portal[3] for the U.S. Department of Health and Human Services, 159 breaches had been reported in 2015 as of the time this column was written. Information on more than 100 million individuals was compromised at some level, not accounting for individuals affected multiple times. If we are not counting duplicates, that is nearly one-third the population of the United States. The most common breach scenario involves paper and films; almost 177,000 records were compromised. Hacking, on the other hand, compromised over 97 million records—more than all the other routes combined. It is easy to see why hacking is so dangerous even if individual error is more common—such as losing a laptop, sending an email by mistake, or misplacing a flash drive. Please do keep in mind that only breaches of over 500 records are reported to the U.S. government for publication.

In January, the Association of Corporate Counsel released its 2015 survey of chief legal officers (CLOs), amounting to nearly 1300 respondents from 46 countries. More than a quarter of CLOs reported that their company had experienced some form of data breach in the preceding 2 years. One notable commonality among the largest breaches, such as those affecting Target, Lowe's, and Goodwill Industries, is that a vendor's actions were the root cause: compromised credentials, data backed up to an unsecure server, and so on. Thus, one obvious lesson from notable breaches is to ensure that your entity has an efficient, effective vendor-management program in place for business associates.

The Cost of a Data Breach

If you are in the health-care industry and you think that your privacy officer is crying wolf, you are sadly mistaken. The cost of one hacking breach, such as the one at MIE that affected patients seen by more than 50 medical providers, can be incredibly high. Interestingly, Symantec now has an online tool that can approximate your cost of a data breach.[4] Once you select your industry with the tool, the first question is about your privacy program. When you complete this questionnaire about a potential hacking of an "average" urgent care center (United States only, fewer than 500 employees, up to 5000 patients, etc.), the tool tells you that on the basis of your input and Symantec's trend data, your center's risk exposure is as follows:

- Companies in your industry with your risk profile have a likelihood of 9.8% of experiencing a data breach in the next 12 months.



K Royal, JD, CIPP/E, CIPP/US, is a former registered nurse turned attorney and compliance professional with 20 years of experience in health-related fields and skilled in privacy laws, breach management, compliance, training, and program development.

- Your average cost per record is $199.
- Your average cost per breach is $597,333.

That's a staggering cost per breach of nearly $600,000, but one with a likelihood of occurrence of less than 10%. When I completed the Symantec questionnaire, I did provide information that the entity had a dedicated chief information security officer and that data could be accessed only by a corporate-owned device that was encrypted. Many health professionals do check email on with their own devices, and most phones are not encrypted. However, changing the parameters by type of breach and device does not change the numbers significantly.

Your organization may be able to survive such a breach by the numbers alone, but can it survive harm in the news media and damage to your reputation? Will you lose the trust of your patients? If you take the right steps, you might keep their trust, especially if you have a long-standing relationship with them. But that is not always the case in the urgent care setting.

The Ponemon Institute found that of all industries, health care has the highest data-breach cost per record, at $363. According to Larry Ponemon, PhD, chairperson and founder of the Ponemon Institute, three factors have contributed to the rising cost of data breaches: an increasing in the number of cyberattacks, the cost of losing customers after a breach, and post-breach response (forensics, crisis team, etc.).

Enforcement, Regulatory Oversight, and Civil Suits

Aside from cost, entities also have to worry about the enforcement actions from both state and federal agencies, along with regulatory oversight—and lawsuits from patient class actions.

Federal

Certainly the Office for Civil Rights (OCR), of the U.S. Department of Health and Human Services, will be interested in your data breach. In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, went live with an interim breach notification rule enacted on September 23, 2009. Subsequently, the HIPAA Omnibus Rule implemented the final rules under HITECH in 2013, which included the removal of a subjective determination of whether the breach caused a "significant risk of financial, reputational, or other harm to the individual." Under the new standard, it is presumed that harm has occurred and the entity must conduct a thorough risk analysis to determine whether risk has occurred. The Omnibus Rule also made HIPAA (and breach notification) applicable to business associates.

Once the OCR has been notified that a breach has occurred, it will contact you for more information about the breach as well about your policies and practices. It is best to cooperate with the OCR, because stonewalling the federal authorities usually increases your cost without noticeable benefits. You should have a breach response team in place, and this team should also assist in the regulatory review process. However, you should have one specific person authorized to respond and communicate in a general sense to reduce any delays.

State

In addition to federal requirements for responding to breaches, there are state requirements. Forty-seven states, plus the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have data breach notification laws.[5] Some are based on simple acquisition of unauthorized individual data, whereas some states require actual access. Notably, Indiana, New York City, Wyoming, and the District of Columbia do not provide a safe harbor for encryption. Thus, although your breach may not require notification under HIPAA, it may still require notification in these areas.

Note that on a state level, there is often notification of various agencies such as those for consumer protection, state attorneys general, and insurance commissions. In fact, some state requirements may contradict others. For example, Massachusetts specifically prohibits notifying individuals of "the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use."[6] State data breach laws may cover both electronic and paper records and apply to more than health records. This is a concern when the data breach may involve employee data, but not patient data. States also generally provide for a private right of action, and state attorneys general are becoming more active in seeking penalties for data breaches.

The good part about state data breach laws is that there is often an exception for entities that are governed under another data breach requirement, such as HIPAA or the Gramm-Leach-Bliley Act of 1999 (for financial services).

Oversight

Oversight in both federal and state actions includes penalties and corrective action plans. At times, the penalties have been quite large:

- **St. Elizabeth's Medical Center in Brighton, Massachusetts:** Employees used an online document-sharing service to distribute patient information. Penalty: $218,400 and a corrective action plan.[7] Note: the complaint was received in November 2012, and the settlement occurred in July 2015.
- **Parkview Health System in Fort Wayne, Indiana:** Medical records in boxes were delivered to a retired physician but were left in her driveway when she was not at home.[8] Penalty: $800,000 and a corrective action plan. The complaint was filed in June 2009, and the settlement came in June 2014.

- **Concentra Health Services in Addison, Texas:** An unencrypted laptop was lost. Penalty: $1,725,220 and a corrective action plan. The laptop was reported to OCR in December 2011, and the settlement occurred in April 2014.

Note the elapsed time between the occurrence or notification and the settlement in all those examples. Years can pass. If the key person at the organization is no longer there or memories fall short, the entity may lose valuable evidence of compliance. Documentation, documentation, documentation.

Lawsuits

In general, lawsuits seem terrifying, but they rarely amount to much in court. The laws have not kept pace with technology to recognize a loss of privacy or to recognize that the steps that people take to protect themselves constitute a harm in and of themselves (with some rare exceptions).

However, that does not mean that the lawsuits are not a threat to entities. Once a suit is filed, the entity generally has to involve outside legal counsel and insurance—and there is generally a settlement. Since 2011, lawsuits for breaches have decreased in number but increased in magnitude, and they more often involve name-brand global companies (Target, Neiman Marcus, Home Depot, Adobe) than health-care entities. A 2014 study of data breach lawsuits[9] found, among other things, that

- Of data breach lawsuits, 76% are filed as class actions.
- Of the 230 cases studied, plaintiffs prevailed only twice, receiving a favorable ruling from a judge or jury.
- The settlement rate is about 50%.
- Breach of medical data was most strongly correlated with settlements.

Practical Steps

In the face of such statistics, some actions can help lessen the cost when a data breach occurs. Entities can be both prudent and practical.

Preparation is key. You have already had some form of data breach, whether reportable to authorities or not. Your employees might not have even alerted you—perhaps a laboratory report went to the wrong patient or a claim went to the wrong insurer. It happens daily. I know. It is likely that one day, you will have a major data breach that requires notification to authorities and individuals impacted. Prepare for that day as if you have been told that it is scheduled to happen next week. Prevent it if possible. If you have a portable device that is not encrypted, then encrypt it. There are free programs for doing so. Assign a separate password to everything—one that is not easy to remember or written on a sticky note stuck to a laptop. There are easy steps to take, and then there are the harder steps, those that a prudent business would take in the face of significant warning signs:

"Preparation is key. You have already had some form of data breach, whether reportable to authorities or not. Your employees might not have even alerted you."

- Involve the executives and board of directors (if you have the latter).
- Get cyber-liability insurance (with direct and indirect cost coverage, and with required and voluntary notifications).
- Have a business-continuity plan and a disaster-recovery plan, and test them.
- Develop a fast and accurate breach response plan (to contain a breach, investigate, and notify all parties), and test it.
- Appoint a privacy officer who really knows privacy and who has authority to act.
- Appoint an information security officer who knows security and who has authority to act.
- Conduct frequent and meaningful security training for employees.
- Oversee your vendors closely.

These steps cannot guarantee that you will not have a megabreach, but they can reduce the chance and reduce the cost when it happens.

References

1. Ponemon Institute. 2014: A year of mega breaches. Traverse City, MI: Ponemon Institute; © 2015 [cited 2015 September 9]. Available from: http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf
2. Information Is Beautiful. World's biggest data breaches. Selected losses greater than 30,000 records. Information Is Beautiful; © 2013 [updated 2015 August 6; cited 2015 September 9]. Available from: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
3. Office for Civil Rights. Breaches affecting 500 or more individuals. Washington DC: U.S. Department of Health and Human Services [updated 2015 September 1; cited 2015 September 9]. Available from: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
4. Symantec. Data breach calculator. Mountain View, CA: Symantec. Available from: http://www.databreachcalculator.com/Calculator/
5. Mintz Levin. State data security breach notification laws. Boston, MA: Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.; © 2009–2015 [updated 2014 January 1; cited 2015 September 9]. Available from: http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (See also National Conference of State Legislators, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, for information on other laws, including other privacy laws.)
6. Massachusetts General Laws §93H-3(b). © 2015 [cited 2015 September 9]. Available from: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section3
7. Office for Civil Rights. Bulletin—HIPAA settlement highlights importance of safeguards when using Internet applications. Washington DC: U.S. Department of Health and Human Services; 2015 July 10 [cited 2015 September 9]. Available from: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/SEMC/bulletin.pdf
8. U.S. Department of Health & Human Services. $800,000 HIPAA settlement in medical records dumping case [press release]. Washington DC: U.S. Department of Health and Human Services; 2014 June 23 [cited 2015 September 9]. Available from: http://www.hhs.gov/news/press/2014pres/06/20140623a.html
9. Romanosky S, Hoffman DA, Acquisti A. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*. 2014;74:1–31. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461