Bloomberg BNA

Health IT Law & Industry Report™

Top Five Privacy and Data Security Issues Facing Healthcare Companies


By Jami Mills Vibbert and Thora Johnson

Jami Mills Vibbert is a member of Venable's Privacy and Data Security practice who advises and counsels clients on matters related to data security, data protection, and data risk management.

Thora Johnson co-chairs Venable's Healthcare Initiative. She provides counsel on regulatory, compliance, tax, and business matters impacting healthcare providers, hospitals, continuing care retirement communities, health insurers, group health plans, pharmaceutical and medical device companies, and digital health companies.

No two health care companies are alike, but many face similar challenges when managing their data risk. Many of these challenges arise due to the competing desires with which every modern organization now struggles—one between innovation and growth on the one hand and compliance and legal risk on the other.

Specifically, the following five issues are top of mind:

1. The tension between data growth and analytics and data minimization;

2. Handling connected devices and mobile apps;

3. Creating effective cross-functional privacy and security teams;

4. The data implications of acquisitions; and

5. Effective and tiered vendor management.

We discuss these issues and offer practical guidance on each.

1. To Big Data or Not to Big Data

Monetizing data is on the mind of every organization looking to outpace competitors and grow revenue. Worldwide revenues in big data and data analytics are expected to grow 50 percent by 2019. (Louis Columbus, Roundup of Analytics, Big Data & BI Forecasts & Estimates, 2016, Forbes (Aug. 20, 2016)).

And 70 percent of organizations say that big data is of critical importance. (Big Data Executives Survey 2016, NewVantage Partners (2016)).

In health care, big data can mean improving patient outcomes (improving services), a better understanding of the clinical services in demand and in what areas (creating efficiencies), and more successful payer performance (higher revenues). This means that the business of healthcare is pushing for more data and more analysis of that data.

It also means that legal and compliance have significant concerns regarding the proliferation of data, in particular any protected health information ("PHI"). Any electronic PHI aggregated, but not de-identified, and analyzed in a new system or location is subject to the same administrative, technical, and physical security controls under the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule as the system from which that data originates.

The more places ePHI exists, the more systems an organization has to maintain and protect as sensitive information and for which it must assess and audit annually. Even more, the duplication of data leads to a new location and therefore a new opportunity for a vulnerability or data loss or breach from that location.

Privacy issues also abound. The health care organization must have the right under HIPAA and its business associates agreements or seek the written authorization of the patients to use and disclose the data in the way contemplated.

If a health care organization outsources data analytics, or even uses a third party cloud service provider to host the data, the "sharing" of this data with the third party must be pursuant to a properly constructed business associates agreement.

The risks of big data can be mitigated by stripping the PHI of all of its 18 statutory identifiers prior to aggregating and analyzing it. If completely de-identified in this way, the data will no longer be considered PHI and will no longer be subject to the privacy and security provisions of HIPAA and many state laws.

If the business desires to maintain one or more of the 18 identifiers that will disallow complete de-identification, communication is key (and see forming a cross-functional team below).

First confirm you have the right to use the data in this way. Then discuss the business need and revenue expected to be generated by this use of the data, and tell the business the risks of using this data in this way.

Work with the business to determine whether the risk and cost of HIPAA compliance is outweighed by the contemplated use. This determination should be made with respect to all data, but is more critical in the case of PHI, where a loss or misuse could cause significant reputational harm, litigation risk, and regulatory involvement.

If justified by the revenue or business goal, ensure in advance of contracting that third party service providers will be willing to sign a Business Associate's Agreement and have an established practice of doing so.

2. The Internet of Medical Things

As with big data and data analytics, health care organizations, like other industries, are trying to and becoming more and more connected. Some forecasts expect $1 trillion in spending on health care Internet of Things ("IoT") by 2025. (J. Manyilea, M. Chui, et al., McKinsey Global Institute, Unlocking the Potential of the Internet of Things (June 2015)).

Connected medical devices and accompanying applications provide the opportunity for organizations to provide innovative, new services to their patient populations. These devices also have the ability to provide additional insight into healthcare services by providing new types of data or access to more of that type of data.

The privacy and security issues with medical IoT devices can be dramatic. Legislatures and regulatory bodies alike have focused significantly on the potential issues of connected devices.

A lack of reasonable data security could lead to oversight by the Federal Trade Commission and/or the Food and Drug Administration ("FDA"). If the security vulnerabilities are significant enough, it could lead to litigation risk as the result of a product defect and its effect on the user of the medical device.

Either regulatory or litigation risk, or even just the discovery of a security flaw, could lead to an expensive recall of the device itself. In addition, the data sharing and privacy issues with respect to devices overlap with those discussed above.

Addressing the security issues of connected devices begins with privacy and security by design.

The business, the developers/engineers, information security, and the lawyers should work together to develop a plan regarding what types of data the device will collect and with whom it will share that information and how.

The mechanism by which consent and authorization will be received for that collection and sharing should be contemplated.

On security, that same team should come together and discuss where the data will be stored and how that system will be protected, how to protect the data in transit to that storage location, how access to that data will be limited both internally and externally, how to monitor vulnerabilities in the device and attacks on and threats to the device, and how the device will be updated and patched.

3. It Takes a Village

One of the buzz words thrown around the most often in privacy and security, but one of the hardest to deploy, is to maintain a privacy and security " culture."

Privacy and security is not just the province of the lawyers, the Chief Information Security Officer, the information technology team, or information security professionals.

Privacy and security cannot function efficiently and effectively either alone or together unless and until a broader cross-functional team that includes the business is dedicated to thinking about and handling privacy and security.

That team, and the organization as a whole, requires appropriate buy-in and oversight at the level of the senior executives or Board of Directors. Easy to say that training and governance are key, but what type and how?

First, make your training directed and interactive. Training should be developed for the different types of employees and contractors your organization has and in connection with the types of data to which those employees have access.

This allows your training to be short enough to be targeted to the real privacy and security issues faced by that group of users. Training should also be interactive—most employees want to do things to protect the reputation of the organization and the privacy of the patient data and confidentiality of the proprietary data being held by that organization.

Interactive training allows back and forth communication among the different divisions within the organization. Create and distribute weekly or monthly tips directed at a new or reminder privacy and security issue facing the organization.

Second, privacy and security professionals should work together and with each other, not against each other, to have the most effective and efficient team. The privacy and security professionals should have open and constant lines of communication on a daily or weekly basis.

While privacy and security do not always overlap, sometimes privacy can solve security problems and sometimes security can solve privacy issues, and thus communication is key.

Along with them, create a cross-functional team in the information security and privacy policies drafted by the company that is comprised not only of the privacy and security professionals, but also other relevant individuals from legal, finance, marketing, human resources, information technology, and the various business units or locations.

Encourage communication among the cross-functional team by requiring monthly meetings of those teams and testing of those teams effectiveness through tabletops or otherwise.

Just like with respect to the privacy and security teams, those teams must work with the business and not against it—privacy and security can improve the product or service and does not always need to say no (nor should it be perceived to always say no).

The risks must be completely understood and accepted by the business when the benefit outweighs the risks, and true cooperation and understanding is needed for this to occur.

Finally, create a team of senior executives or a committee of the Board to oversee and provide accountability for the privacy and security teams.

Draft a charter for that team or committee, require meetings by procedure or policy, and require reporting by the cross-functional team to the oversight committee semi-annually at a minimum.

4. Grow Smartly

Acquisitions in health care are common as hospital systems continue to consolidate. One thing not contemplated enough in the acquisition of an organization concerns data.

Prior to engaging in negotiations concerning the acquisition of a company, the organization should determine the potential impact that a latent breach at the target company would have on the cost of that company and the reputation of the organization purchasing that company.

Once a purchaser has considered the potential impact of a breach, it should use that knowledge to conduct due diligence.

Depending on the risk posed, the due diligence could consist of conducting a cybersecurity risk assessment on the target, a management call or meeting at the target, asking detailed questions concerning the company's security posture and policies, or even a full cybersecurity assessment that includes a thorough review of the policies, procedures, and controls of the company, interviews of employees and management, technical vulnerability testing, and an assessment of the company's compliance practices with the industry's best standards and any relevant regulatory requirements.

Remember, when a company is bought, its data is bought, and must be addressed. For example, if the target will be discarding its financial information system and joining the purchaser's, migrate any necessary data (which may constitute ePHI), but do not maintain the legacy system.

This information poses a security risk (the more places information is located, the more places it can be stolen from), and additionally poses a risk that it will become the subject of litigation and then becomes costly to review and produce what was at one time unnecessary information to retain.

If an acquisition does occur after the diligence process concludes, consider whether to take the data of the target, or, more importantly, which data. That decision should be made by determining what data is necessary to grow the business or revenue of the purchaser or to continue necessary operations at the target.

There should be an investigation into whether the acquiring company has the right to acquire that data. And then, most importantly, delete and securely dispose of any information that does not need to be maintained for business continuity, regulatory retention, litigation hold, or revenue-generating purposes.

5. Share the Work, and the Risk

All health care organizations rely extensively on third parties to provide essential services.

Many of these third parties are accessing sensitive data or systems containing that data. Pretty straightforward. But before allowing those third parties to access or store your data or systems, ensure the appropriate vendor management program is in place.

Conduct due diligence on the third parties—just as with acquisitions, conduct that due diligence in a tiered fashion. Slightly different here, management calls are likely not necessary or available, but tier the questionnaires to the risk that particularly third party poses.

For example, if the third party maintains a certification from a well-recognized security organization, many of the due diligence questions may be unnecessary. Alternatively, if the third party will be accessing or storing only relatively non-sensitive information, perhaps only basic questions regarding security are necessary to begin the engagement.

Just as important, however, are the contractual provisions necessary to share the risk once the organization has decided to move forward with the engagement. These contractual provisions include representations and warranties specifically related to privacy and security.

Organizations should decide what type of ongoing monitoring of security practices it needs based on the vendor including whether it needs (and wants) an audit right.

Indemnification provisions and liability caps should contemplate business-to-business and third party claims for a loss or misuse of information. Whether and the type of insurance must be accounted for, particularly if the organization is small or otherwise may not be able to cover the true costs of a data loss.

Depending on the jurisdiction and the nature of the contract, the location of the information (i.e., where the servers holding the data will be located or to which jurisdictions the data may be transferred) must be negotiated.

This complex process, and third party privacy and security risk management, not only protects the organization vis-à-vis the contracting party, but also against regulatory and litigation risk for failing to adequately oversee its third parties (which will be considered as inadequate or unreasonable security by many regulatory bodies).

While privacy and security issues often increase as innovation or growth increases, thoughtfulness throughout the process specifically directed at these issues can drastically reduce the risk associated with the benefit of this growth. Above, we have listed some of these practical steps to take.