Volume 2, Issue 12 December 2015

Population Health NEWS

Revolution From Healthcare to Self-Care

by Ted Spooner

Not that long ago, if consumers wanted to make a deposit in a bank account, they needed to go to a bank. If they wanted to withdraw or transfer funds, they could only do it during banking hours, wait in a line for the next teller and hope for the best. If they needed to do any of these things on a weekend or holiday, tough luck; it's not going to happen. Then in the 1990s, the online banking revolution transformed the banking experience, giving consumers easy access to their money 24 hours a day, seven days a week.

This "self-service revolution" transformed consumer finance and the banking institutions that deliver it. With the advent of consumer-facing, healthcare innovation, a similar transformative consumer experience is set to revolutionize healthcare. Is healthcare prepared for what could be a "self-care revolution"?

Healthcare and financial institutions share a similar mindset. They both enjoy what is called a "social charter." While both generate substantial revenues and in different business forms are either for profit or not-for-profit, they both serve populations for which they have a high degree of responsibility. Bank customers trust that banks will keep their money safe, and healthcare consumers trust their healthcare provider will give them the best care. These institutions are charged with this responsibility under great scrutiny in a heavily regulated environment that demands compliance with rules and laws.

(continued on page 4)

In This Issue

The Road to HIPAA Compliance

by Egor Kobelev

Although the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules successfully protect individuals' private healthcare information, remaining compliant is not without its challenges. The rules contain requirements for any organization that operates using electronic-protected, health information (PHI), including business associates, covered entities, subcontractors and anyone with access to patient information that provide support in treatment, payment or operations. If organizations do not comply, they could face fines, criminal charges and damage to their reputations.

In trying to become HIPAA compliant, it takes more than just having compliant software; the real trick is understanding that HIPAA compliance is not a destination but a long journey of continuous improvements, including those in company operations and procedures. Having related healthcare experience is invaluable to helping an organization become HIPAA compliant.

HIPAA compliance implementation is not a straightforward exercise; however, a large portion of its complexity resides in the very first step—planning. There are as many approaches to the process as the number of companies seeking to achieve compliance. Approaches heavily depend on the type of company—hospital, health plan, insurance company, clearing house, third party administrators—as well as on their specific needs and goals. Working with a team experienced in specific types of HIPAA compliance implementation is critical.

When it comes to planning, organizations should turn their attention to three areas that are affected by HIPAA, roughly defined as process, infrastructure and technology.

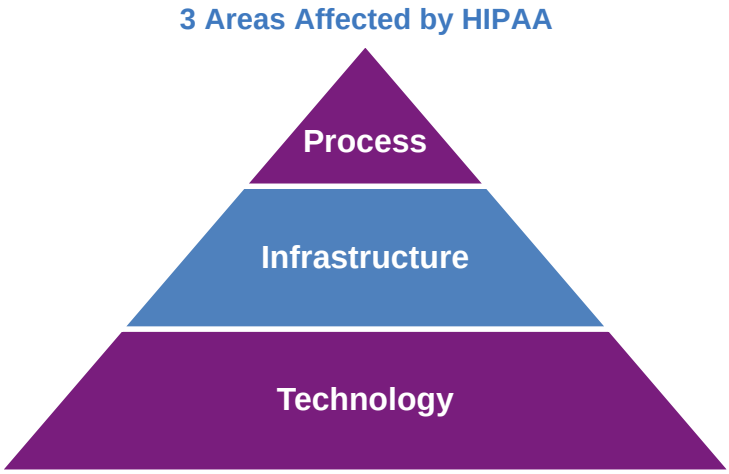
1. **Process.** The cornerstone of HIPAA compliance is all about the process and paperwork. Not only should business processes in an organization be in line with HIPAA law, but they also have to be properly documented as HIPAA Standard Operating Procedures (SOP). SOP should reflect a company's operations, which in turn should comply with SOP. What makes things especially complicated is that relying solely on a human resources (HR) department to drive change is not sufficient; instead, it is important to ensure cooperation between HR and information technology departments. A trusted technology consultancy could be particularly helpful in boosting collaboration, facilitating communications and helping with risk analysis and risk management.

(continued on page 7)

The Road to HIPAA Compliance ... *continued from page 1*

The following are some of the specific steps that need to be taken down the road:

- **Designate a privacy officer**, someone who ultimately would be responsible for the security of PHI and ensure organizational adherence to mandatory security management processes. This person should be able to deal with technical issues involved and effectively interact with other members of an organization to accomplish security rule compliance.
- **Develop and enforce SOPs**. This task typically lies with an HR department, but it would definitely benefit from IT input. The HIPAA Security Rule requires several policies to cover areas including training; identifying, reporting, investigating and responding to security breaches; penalizing employees for security violations, including access to PHI and proper data destruction; and proper handling of terminated employees.



- **Update business associate agreements (BAAs)**. Each BAA must require that a business associate implement safeguards for PHI to ensure subcontractors operate under the same rules and report any known security breaches to a covered entity.
- **Establish contingency planning**. The security rule requires planning for contingencies that might affect the integrity or availability of data. To that end, organizations must create and maintain data back-ups, be capable of restoring lost data and establish safeguard policies and procedures, while still maintaining access to PHI when operating in emergency mode.

2. **Infrastructure.** HIPAA compliance heavily depends on a company's IT and Infrastructure. It is quite rare nowadays for a company to build and run its own data center. It usually requires a fair amount of upfront investment and maintenance costs. In some situations, it makes sense to go this way as it gives the company total control over PHI data; however, this requires that the infrastructure be built so that none of the components violate HIPAA. If a company is hosting data with a HIPAA-compliant, hosting provider, it must have certain administrative, physical and technical safeguards in place.

   Cloud technologies and hosting offerings come with a security concern. Using the cloud means decreased control over data, access to it and even its physical location. Early cloud offerings did not support HIPAA requirements at all, and some still don't. Choosing a hosting partner in line with HIPAA and following through with the execution of BAA require serious consideration.

   "Cloud technologies and hosting offerings come with a security concern. Using the cloud means decreased control over data, access to it and even its physical location."

   For example, a provision in newer BAAs is one that would allow a cloud vendor to use an organization's de-identified patient data for its own use. An industry is developing around the aggregation of data for purposes such as research or predicting patient outcomes. Some business associates are moving toward capitalizing on data, either using them or marketing data to others. While there is nothing wrong with this—as long as the data are properly de-identified—organizations need to be cautious about granting business associates permission to use data in this manner.

3. **Technology.** In comparison, this is one of the easiest steps: developing software in accordance with HIPAA Privacy and Security Rules whose requirements have technical implications. To achieve this, it is necessary to maintain internal technical guidelines and facilitate training sessions for engineers and management involved in the compliance process. Every software product has to be certified upon release and then again following each significant change or update. Organizations have to demonstrate compliance on an annual basis. As the industry develops, companies need to make sure that they react properly to changes in the environment.

   For example, telemedicine is taking a jump forward; more providers are using telemedicine as an adjunct to their operations to treat patients who cannot come to the office, for translation services and to bring more specialized services to a setting. New technologies come with new security concerns that need to be addressed quickly. Technology consultants can help companies ensure that their software is compliant with HIPAA regulations and help simplify the certification process. It's important to have a vendor who is not only capable developing HIPAA-complaint solutions from scratch, but one who also can also take over an existing solution from a client, establish a technical review, modernize a solution and fine tune it so it becomes HIPAA compliant.

Egor Kobelev is engagement manager, healthcare and life sciences, for DataArt, a technology consulting firm based in New York City. Egor can be reached at egor.kobelev@dataart.com.

