WPC™
HEALTHCARE
wisdom.performance.credibility

Remaining Secure in an Evolving Industry

White Paper

Remaining Secure in an Evolving Industry

How Healthcare Organizations Can Manage Risk by Managing Data

Highlights

- A mature data management strategy is the key to staying competitive and staying secure while the healthcare industry shifts to a fee-for-value model.
- Consolidation is on the rise as healthcare companies attempt to manage risk.
- There is considerable room for improvement in the healthcare industry in terms of security.
- Companies must begin with a thorough security assessment to evaluate what measures need implementation.

We live in interesting and exciting times. Our healthcare system is undergoing a massive transformation in which the current fee-for-service reimbursement model is rapidly shifting toward a fee-for-value model with more than two-thirds of payments expected to be based on value measurement in five years—up from just one-third today.[1]

Although the end result of the new fee-for-value model is a more viable system where prices are better controlled and patients benefit from better outcomes, the transition creates significant market disruption. Stakeholders are chasing after Big Data and the insights related to that data. But that strategy has resulted in an unintended liability in terms of data vulnerability. These insights can only be gleaned from the integration and aggregation of diverse data sources and are driving many healthcare companies to consolidate information into a single repository creating an exponentially greater security problem when compared to the prior world where data remained in separated silos. Healthcare organizations must take on more risk, but they are not adequately managing that increased risk, which can threaten the viability of their respective businesses.

The correct approach to successfully operating in this new fee-for-value world is two-pronged: organizations must invest in data maturity *and* focus on security. By creating an environment in which data are normalized, companies can better compete and operate in an evolving industry. And with a comprehensive data security strategy in place, organizations are free to focus on moving forward without the risk of breaches that would put patient records in jeopardy and pose the risk of significant fines—not to mention publicity disasters.

Current Trends as the Industry Attempts to Manage Risk

One consequence of the evolving reimbursement models has been an increase in consolidation in the industry. This has not typically been in the form of competitors buying each other but rather complementary pieces coming together—providers buying payers, payers buying technology companies, and technology companies vertically expanding their services—all in the name of better managing risk and, to a lesser degree, acquiring the talent needed to transform their business.

While merger and acquisition activity dominates the headlines, other business arrangements that are increasing in popularity include affiliations, joint ventures and, to a lesser extent, joint operating agreements. In fact, a 2012 survey revealed that only 13% of hospitals intend to maintain independence from alignment with other hospitals or systems.[2] Said in a different way, the market remains interested in exploring creative ways to align with other organizations for the purpose of managing risk, increasing scale, expanding reach and benefiting from complementary strengths.

Key to the success of these partnerships (particularly clinically integrated networks and accountable care organizations) is the ability to exchange data with stakeholders across the care continuum. And therein lies the challenge.

While much can be gleaned from the aggregation of data from varying parts of the health system, it first requires a level of data maturity (something most participants lack) to ensure meaning can be derived from cross-organization data.

Essentially, the rationale behind these partnerships is that the sum of the parts will generate more value than the individual parts themselves, but this presumes the individual parts are creating value in the first place. In order for this to be true, organizations must first have the ability to glean insight from their own data before truly harnessing the value of using external data to complement their own.

In addition, validating the effectiveness of another organization from a financial, clinical and operational standpoint requires the availability of normalized data. While many organizations are responding to this challenge by aggressively investing in advanced analytics, it is a foolish endeavor to pursue if the necessary investment in data maturity has been overlooked.

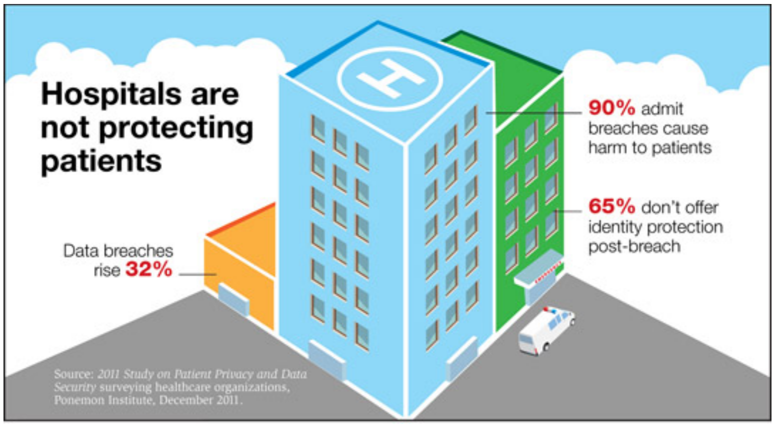
Data Maturity Is the Necessary Foundation

Maturity around data governance is the foundation upon which an effective data strategy is built, and it enables the insights that healthcare executives crave. The process of achieving data maturity involves assessing, managing, using, improving, monitoring, maintaining and protecting organizational information. It is how companies integrate, aggregate, normalize and report on their data.

Data maturity means healthcare companies understand who has access to data, where data lie and how long they are required to store data. Without an effective data governance strategy in place, healthcare companies will struggle to adequately protect patient data.

With data maturity, stakeholders have the ability to draw real insights from data that can create better patient outcomes and contribute to the bottom line.

Healthcare Industry Lacks Adequate Data Security


Hospitals are not protecting patients
90% admit breaches cause harm to patients
65% don't offer identity protection post-breach
Data breaches rise 32%

Source: *2011 Study on Patient Privacy and Data Security* surveying healthcare organizations, Ponemon Institute, December 2011.

Unfortunately, the healthcare industry has a poor track record when it comes to security, and trends indicate that significant effort should be made to enhance data security. The recent Anthem breach affected a whopping 80 million patients. According to medical fraud experts, medical records are 10 times more valuable on the black market than credit card numbers[3] A new study by the Ponemon Institute indicates medical identity theft has increased 21.7% since 2014.[4]

When it comes to email security, the healthcare industry significantly lags, according to a survey released by Agari, an email security company. Analysis of companies' email communications revealed only one, Aetna, adequately attempted to protect customers from email fraud. An email claiming to be from a health insurer is four times more likely to be fraudulent than an email supposedly from a social media company, so the healthcare industry must step up its game to prevent phishing—attempts from hackers to obtain sensitive personal information by sending fake emails.[5]

Despite the obvious interest of hackers in healthcare information, healthcare data security continues to remain a low priority for hospitals, according to a recent survey. Executives cited ICD-10 and population health as areas of focus, and most indicate they are not planning to invest in data security tools in 2015.[6]

Steps to Better Data Security

What are the primary causes of data breaches?

- Lost or stolen computing device (46%)
- Employee mistakes or unintentional actions (42%)
- Third-party snafus (42%)
- Criminal attack (33%)
- Technical systems glitch (31%)
- Malicious insider (14%)
- Intentional non-malicious employee action (8%)

With an adequate data governance strategy in place, healthcare organizations must turn their attention to security by first evaluating where they stand. A thorough security assessment should cover HIPAA/HITRUST and Meaningful Use risk analysis, software security lifecycle development and assessment, audits and security reviews of business associates, and vendor risk assessment. Using information garnered from security assessments, organizations are then able to develop effective policies and governance around security.

With proactive security measures in place, hospitals and payers can achieve regulatory compliance, reduce IT and security risk, maintain business continuity, and lower costs.

It's not a matter of "oops, sorry," because serious data breaches come from a variety of sources both intentional and unintentional, internal and external, criminal and innocent. But who wants to explain to patients why their data have been compromised? Every breach is serious, no matter the cause. And who discovers the breaches? One source says about half are found through audits; nearly half are found by employees; and a third come from patient complaints.

The Right Partner for Security and More

As the original contractor to CMS for HIPAA compliance, WPC Healthcare is ideally suited to address the security needs of healthcare organizations. With expertise in HITRUST, HIPAA, DEA EPCS, CFR 21, Red Flag Rule regulations and more, WPC has a successful track record of supporting healthcare companies with IT disaster recovery and recovery of clinical and administrative applications including EHR systems.

Furthermore, WPC has built a solution set that supports organizations in developing a data maturity capability regardless of where they are in the continuum today. More than 40 years of data expertise makes WPC the right partner to assess and address issues with underlying data sources. This process positions clients for success and prepares them to seize the opportunities presented from the ongoing changes in the industry.

With effective data maturity and security strategies in place, healthcare organizations are positioned to not just survive in an evolving industry, but thrive.

To learn more about WPC, contact us at 615.913.8850 or info@wpchealthcare.com, or visit us online at wpchealthcare.com.

[1] *The 2014 State of Value-Based Reimbursement*, an independent research study of 464 payers and providers conducted by ORC International.
[2] Media Intelligence, M&A: Hospitals Take Hold, January 2012.
[3] Caroline Humer and Jim Finkle, "Your Medical Record Is Worth More to Hackers Than Your Credit Card," Reuters, September 24, 2014.
[4] Stephanie Reardon, "Medical Identity Theft Increases 21%, Says Ponemon Study," *Health IT Security*, February 23, 2015.
[5] Robert Hackett, "Health Companies Flunked an Email Security Survey—Except Aetna. Why?" *Fortune*, February 19, 2015.
[6] Elizabeth Snell, "Healthcare Data Security Not Major Priority For Hospitals," *Health IT Security*, March 5, 2015.