

# Health Information Technology: The Imperative of Risk and Compliance Management in the HITECH Age



A Frost & Sullivan White Paper

**TABLE OF CONTENTS**

**PROMOTING THE ADOPTION OF HIT AND PROTECTING PRIVACY:  
HITECH AND MEANINGFUL USE ..... 3**

**HEALTH INFORMATION EXCHANGES..... 7**

**PROMOTING COLLABORATIVE CARE MODELS..... 7**

**THE RISKS OF FLUID INFORMATION ..... 7**

**DIGITIZED ORGANIZATIONS REQUIRE CONTINUITY OF ACCESS ..... 9**

**THE BENEFITS OF IMPLEMENTING A RISK AND COMPLIANCE  
MANAGEMENT STRATEGY ..... 9**

**THE STEPS TO MANAGING RISK AND COMPLIANCE ..... 10**

**EXAMPLES OF STRATEGIES FOR MANAGING RISK AND COMPLIANCE.. 13**

**CONCLUSION ..... 13**

**ACRONYMS AND DEFINITIONS..... 14**

Health information technology (HIT) is believed by most policymakers, health professionals, and other stakeholders to be the best means of improving patient safety and health, increasing healthcare efficiency, improving resource utilization, and lowering healthcare costs. But HIT also raises concerns about the privacy and security of personal health information. As the United States and other nations grapple with healthcare quality and unsustainable costs by promoting HIT, health information exchanges, and collaborative care models, sensitive health information is becoming more vulnerable. Information that previously remained on paper and accessible only to the healthcare provider and staff who produced it will increasingly flow electronically among providers, within and outside a hospital's walls, and between providers and other stakeholders, such as payers. HIT creates fluid information, enabling more people to access and alter private health information and creating more issues for providers and payers in managing risks and compliance.

In this paper, we review:

- Initiatives to encourage the adoption of HIT,
- Health information exchanges (HIE) and collaborative care models,
- The risks and compliance issues emanating from HIT, HIE, and collaborative care models,
- The need for data continuity in the world of digitized healthcare information,
- The necessity of implementing a risk and compliance management strategy,
- Essential steps in designing any risk and compliance management strategy, and
- Examples of strategies and technologies for managing risk and compliance.

Healthcare executives, providers, payers, and their business associates must deal with risk and compliance management from the very beginning of HIT development or face potentially serious consequences: poorer health outcomes, ruined reputations, and financial losses from security breaches, lost data, and noncompliance.

## **PROMOTING THE ADOPTION OF HIT AND PROTECTING PRIVACY: HITECH AND MEANINGFUL USE**

Many governments have adopted proactive initiatives to encourage the adoption of HIT. In recent years, the European Union (EU) has begun to realize the benefits of adopting HIT, resulting in several programs such as *Ten4Health* in the EU<sup>1</sup> and the *2012 Hospital Plan*<sup>2</sup> in France. In January 2009, China announced a U.S. \$124 billion stimulus package over the next three years to reshape the nation's healthcare system, including the modernization of services with digital hospitalization, *electronic medical records* (EMR), and next-generation information networks. In Canada's 2009 budget, C\$500 million was invested in the non-profit Canada Health Infoway to develop and implement e-health technologies throughout the country.

The U.S. government is pushing the adoption of HIT through both incentives and disincentives. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA) of 2009, allocates billions of dollars to providers for adopting and using, in a meaningful way,

electronic health records (EHR). Additionally, it enhances privacy and security measures in the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

What does HITECH mean for providers, patients, payers, and business associates of providers? One, it provides the financial incentives necessary to convince providers to adopt and use EHR. While there is convincing evidence that HIT such as EHR will save money, the initial costs of establishing an infrastructure are high.<sup>3</sup> In 2005, the Rand Corporation noted that those who must bear the costs of HIT—providers—are often not the ones who realize its cost-savings and recommended the government establish incentives.<sup>4</sup> HITECH incentives are one means of doing so. Providers who adopt HIT and demonstrate *meaningful use* (MU) of it in their medical practices will receive financial incentives. While the criteria for establishing MU have not yet been defined, it means providers must show they are “using certified EHR technology in ways that can be measured significantly in quality and in quantity.”<sup>5</sup>

First, in order to meet Meaningful Use requirements to receive HITECH financial incentives, healthcare providers must be able to exchange meaningful healthcare information with other healthcare professionals. This means patient data must be able to be moved outside the provider’s protected network.

Second, HITECH places greater responsibility and accountability on providers and their business associates for ensuring *protected health information* (PHI) is secure and remains private. PHI is individually identifiable information in any form—digital, paper, oral—stored or transmitted by a provider or its business associates. Individually identifiable information includes any information on mental or physical health, the provision of healthcare, or payments for healthcare. Table I compares significant changes in HIPAA regulations prior to and since HITECH.

---

<sup>1</sup> The *Ten4Health* project established a secure Web service integrating HIT infrastructure networks in EU member countries. The service has been vital in enabling EU citizens to receive medical care while in other EU nations using the European Health Insurance card and paves the way for using the forthcoming eCard version.

<sup>2</sup> The *2012 Hospital Plan* allocates €1.5 billion for HIT investments in France.

<sup>3</sup> In a 2005 synthesis report of research on HIT, the Rand Corporation found that the savings from efficiency alone could be more than \$77 billion, and health and safety benefits could double that savings while reducing morbidity and mortality. Source: Rand Corporation. 2005. “Health Information Technology: Can HIT Lower Costs and Improve Quality?” RAND Health: Research Highlights. Santa Monica, CA: Rand Corporation.

<sup>4</sup> *Ibid.*

<sup>5</sup> CMS. 2010. “Meaningful Use.” [http://www.cms.gov/EHRIncentivePrograms/30\\_Meaningful\\_Use.asp#TopOfPage](http://www.cms.gov/EHRIncentivePrograms/30_Meaningful_Use.asp#TopOfPage) (April 6, 2011)

**Table 1: HIPAA Compliance Regulations and Noncompliance Penalties Prior to and After the HITECH Act**

|  | HIPAA before HITECH  | HIPAA after HITECH   |
|--|--|--|
| Definition of Business Associates (BA) | Health plan, clearing house, or provider involved in the disclosure of PHI             | Expanded to include health information exchanges, collaborative care organizations, businesses and subcontractors having access to PHI   |
| Are BAs Subject to HIPAA Compliance?   | No, except within contractual agreements with covered entities                         | Yes. Security Provisions and Penalties now apply. Now directly responsible and liable for breaches.  |
| Data Breach Notification               | Not obligated to notify patients of breaches, except under state mandates              | Must notify HHS of all breaches; give written notification to affected individuals no later than 60 days from discovery of breach; notify media of breaches involving more than 500 individuals in one state or territory  |
| Data Breach Enforcement                | Collaborative resolution of noncompliance; applies to covered entities not individuals | HHS Office for Civil Rights conducts complaint investigations and compliance reviews; also applies to individuals, employees, and BAs; HHS must report to Congress on complaints and resolutions   |
| Civil Penalties for Data Breach        | \$100 per incident; \$25,000 cap per calendar year                                     | \$100 to \$50,000 or more per violation; \$1.5 million cap per calendar year   |
| Criminal Penalties for Data Breach     |  | Up to \$50,000 and 1 year imprisonment for knowingly disclosing PHI; up to \$100,000 and 5 years imprisonment for willful disclosures involving false pretenses; \$250,000 and 10 years imprisonment for willful disclosures for commercial advantage, personal gain, or malicious intent. |

Source: Frost & Sullivan

Since passage of the HITECH Act, it is clear that the HHS Office for Civil Rights and the Department of Justice—the entities responsible for pursuing civil and criminal penalties—are going to enforce compliance regulations. In January 2010, a former researcher at UCLA’s David Geffen School of Medicine became the first healthcare worker sentenced to prison for violating HIPAA privacy provisions. The cardiothoracic surgeon was sentenced to four months in federal prison and fined \$2,000. After receiving notice of his dismissal from UCLA, the surgeon accessed the medical records of his immediate supervisor, other employees, and well-known celebrities 323 times over a three-week period. Acting United States Attorney George Cardona stated:

There is a persistent problem with improper and illegal viewing of medical records by individuals who abuse the access they have as a result of their employment. HIPAA's criminal privacy provisions protect not only celebrities, but all of us from curious neighbors, disgruntled co-workers, and other snoopers.<sup>6</sup>

The surgeon's defense attorney stated that his client, a Chinese national, did not know he was breaking the law, highlighting the importance of training staff. Other heavily regulated industries and agencies have adapted to information technology and the need to conduct annual training of staff to ensure compliance to regulations; it is past time for healthcare to do the same. For example, the Internal Revenue Service requires annual training of employees about privacy, disclosure and unauthorized access of tax returns.

In February 2011, Cignet Health of Maryland was fined \$4.3 million in civil penalties for violating HIPAA privacy regulations. It was fined \$1.3 million for not providing 41 patients with their medical records upon request and another \$3.0 million for its "arrogance" in not cooperating with investigators. They are the first provider to be fined for such a violation. Privacy expert Rebecca Herold stated:

This should also serve as an example and provide good motivation for all covered entities and business associates to get into compliance, and maintain compliance, with HIPAA and HITECH. [Privacy and security officers] need to show this news report to their CEOs and CFOs to prove that penalties not only can occur, but that they have now started, and with quite a big, financially painful bang. Due to their apparent lack of compliance, as well as demonstrable arrogance with regard to dealing with the OCR investigators, Cignet now has the dubious honor of being the poster child for HIPAA/HITECH willful neglect.<sup>7</sup>

And Jeff Drummond, a health attorney in Dallas, stated:

For some time now, many of us who follow HIPAA have been waiting for OCR to find a particularly egregious case and deliver a significant fine, so that some in the healthcare industry who have gotten lackadaisical about HIPAA compliance will sit up and take notice. This may just be the case.<sup>8</sup>

---

<sup>6</sup> FBI. 2010. "Ex-UCLA Healthcare System Employee Pleaded Guilty to Four Counts of Illegally Peeking at Patient Records." <http://losangeles.fbi.gov/dojpressrel/pressrel10/la010810a.htm> (April 6, 2011)

<sup>7</sup> Nicastro, D. 2011. "First civil money penalty for HIPAA Privacy Rule violations." <http://blogs.hcpro.com/hipaa/2011/02/first-civil-money-penalty-for-hipaa-privacy-rule-violations/> (April 6, 2011)

<sup>8</sup> *Ibid.*

## HEALTH INFORMATION EXCHANGES

In order to realize the benefits of HIT, patient health information needs to be shared among patients, providers, payers, and other authorized users within and outside of a provider's walls. Different incarnations of health information exchanges (HIE) have appeared since the 1990s. Community Health Information Networks (CHINs) and Regional Health Information Organizations (RHIOs) are variations that have largely failed because of a lack of value for participants. But HITECH now adds value to exchanges. The HIE Cooperative Agreement Program has funded 56 states and territories to rapidly build capacity for exchanging health information across the healthcare system both within and across states. The grants are to be used to increase connectivity and enable the flow of patient health information. The ultimate goal is to develop interconnected regional exchanges that can eventually connect nationwide. Such an exchange, while necessary to achieve the goals of HIT, vastly expands the risks to PHI.

## PROMOTING COLLABORATIVE CARE MODELS

The HITECH Act also promotes two organizational models for healthcare delivery: patient-centered medical homes (PCMH) and accountable care organizations (ACO). PCMHs coordinate all healthcare for a member patient, with the patient and primary care physician designing the care plan and developing health outcome goals. ACOs are a network of doctors and hospitals that have agreed to provide all healthcare needs for a minimum of 5,000 Medicare patients. The two are not mutually exclusive, and ACOs may embody PCMHs.

These models, if successful, will fundamentally change the way healthcare is delivered in the United States by focusing on patient-centered, preventive care rather than fee-for-service care. But, again, HIT is the enabler of PCMHs and ACOs. Collaborative, coordinated care requires the exchange of patient information, including that obtained from remote monitoring, image-intensive diagnostic and treatment devices, multiple specialists, pharmacies, and so on. PCMHs and ACOs will increase the complexity of HIE, the vulnerability of PHI, and risks of noncompliance.

Additionally, compliance, fraud and abuse, and antitrust issues are amplified. A proposed federal rule on ACOs was recently announced to address some of these issues. ACO patients would have to opt out of having their Medicare claims data shared among ACO providers. Federal authorities are seeking comments on potential risks to PHI and on the use of opt-out rather than opt-in for data sharing. In another proposal, federal authorities are considering waivers of fraud and abuse rules, including the federal anti-kickback statute and the physician self-referral law. And the Federal Trade Commission and the Department of Justice released a proposal that ACOs could fall into antitrust safety zones or receive expedited review.

## THE RISKS OF FLUID INFORMATION

Policymakers and HIT experts are concerned that healthcare organizations are not dealing adequately with security issues as they develop HIT systems. HIT strategies have focused on information access/exchange to demonstrate MU for HITECH funding.

However, it is crucial that hospital systems, providers, and business associates focus on the security risks and compliance issues inherent in a system that involves increasingly fluid private health information.

These issues are compounded by a rise in hospital consolidations and the push for the development of collaborative care models. When hospital systems acquire new sites or health information exchanges are developed, these previously disparate organizations must integrate HIT infrastructures, EHR systems, security, and backup capabilities. Yet HIT funds are typically directed to getting the systems to talk to each other first and then developing risk and security measures last. After all, emphasis is on the clinical and administrative/financial value of HIT.

As connected health systems continue to push the input of information to the edge, with remote monitoring devices that collect patient health information and bring it back to the provider for analysis and storage, the healthcare provider's database is now exposed to the potential for remote access. With an increasing number of applications and devices in use and in development—from wearable sensors, devices that connect through mobile handsets, software applications that reside on or are accessed through smart phones, and stand-alone devices that are placed in the home—a greater emphasis must be placed on software security and remote access. Creation of “Denial of Service” events and commands to extract information from hospital databases are only two of many risks these remote devices could create.

Defense from malicious remote access will be required at all layers: in application design; in the device, hub, and server; and at the firewall.<sup>9</sup> Since many of the businesses developing these connected health solutions are small, innovative organizations, and because their focus is primarily on clinical application and connectivity issues, they have given less attention to security to date.

Risks of data breaches extend to the businesses hospitals and providers contract with to perform vital functions such as medical transcription and billing. These business associates are now held to the same standards as any covered entity within the healthcare organization. If any businesses providing contracted services or their sub-contractors have access to PHI, they are responsible for compliance and are subject to the same civil and criminal penalties as healthcare providers.

Covered entities must pay particular attention to business relationships with offshore companies, because entities based in foreign countries are not bound by U.S. law. If a security breach occurs offshore, the U.S.-based provider is still liable and may have little recourse with the offshore business associate responsible for the breach beyond what is specified in their contractual agreement.

---

<sup>9</sup> The Health Information Trust Alliance (HITRUST), a company devoted to establishing and promoting HIT security standards, currently has a mobile device working group focused on bringing forward security standards within the year for mobile devices and software applications that run on these devices.

## **DIGITIZED ORGANIZATIONS REQUIRE CONTINUITY OF ACCESS**

While data breaches make the news and focus attention on data security, constant and uninterrupted access to electronic patient information is more important to daily hospital operation and patient care. As hospitals move to fully electronic systems, they will not be able to function safely without continuous access to patient data and electronic medical records. This highlights the need for substantial backup and disaster recovery systems to support EHRs and other crucial electronic clinical systems, such as image-intensive medical devices. With the layering of more and more clinical applications, there is an exponential increase in dependence on storage and electronic delivery of patient information.

Imagine the following scenario: A hospital's HIT system crashes and it only intermittently backs it up on antiquated tapes. Emergency room physicians and nurses are unable to access patients' EHRs to guide diagnosis and treatment, the OR has had to cancel surgeries because critical patient information is inaccessible, physicians are not able to prescribe medications because their computerized physician order entry system is down, and essential business operations such as billing and scheduling are impossible. IT failures can take days to restore and lost data may be irretrievable, leaving the hospital unable to provide adequate care.

## **THE BENEFITS OF IMPLEMENTING A RISK AND COMPLIANCE MANAGEMENT STRATEGY**

Taking risk and compliance management seriously is a fundamentally sound business decision. Not only does it make possible all of the benefits associated with HIT in general, but it also protects patients, providers, business associates, payers, and other organizations.

### **Improve patient and customer satisfaction**

Providers depend upon satisfied patients, and business associates depend upon satisfied customers. Trust is the foundation of satisfactory relationships, and trust is achieved by demonstrating privacy is a priority.

### **Reduce the cost of data breaches**

HHS and the Department of Justice have made it clear: noncompliance is expensive. With the advent of HITECH, the ante has been raised to invest in risk and compliance management. Financial incentives for meaningful use, enormous civil and criminal penalties, and prison time have tipped the balance toward wise investment in secure systems.

### **Build and maintain reputation and competitiveness**

Securing your reputation in the healthcare industry is critical to success. Business associates should make particular note of this benefit. If they are unable to assure clients they are HIPAA-compliant and trustworthy handling PHI, they will not get the contracts they need to survive and grow.

### **Promote evidence-based medicine**

EHRs provide a wealth of longitudinal clinical data for analysis of medical treatments and disease trends, but this is only possible when data is shared across providers and with researchers, which requires an assurance that PHI is secure.

### **Improve public health**

Public health systems and programs can be transformed by integrating information exchanges with providers. By developing electronic surveillance and registry systems, providers can streamline reporting, and epidemiologists can identify and analyze disease trends more quickly. This can only be accomplished through secure, HIPAA-compliant systems.

### **Prevent system downtime**

The greatest threat to day-to-day operations is HIT system downtime. Critical decisions are made based upon clinical information collected, analyzed, delivered, and stored electronically. The costs of losing access to vital clinical data are enormous: patients' well-being, the organization's reputation, and malpractice risks.

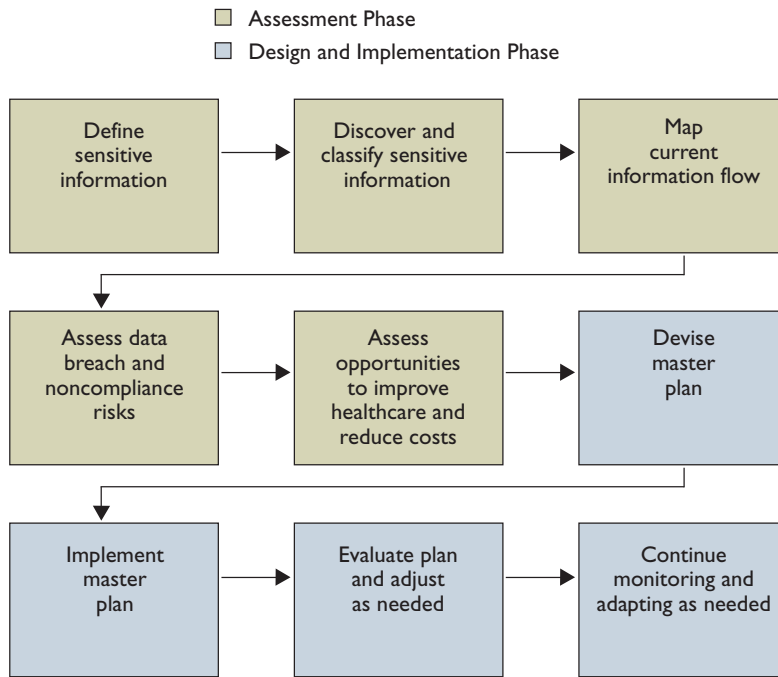
### **Improve contract management**

Investing in quality HIT risk and compliance management also enables providers and hospital systems to streamline and monitor contracts. As patient care becomes more collaborative, the number of contracts to manage these relationships will grow. A well-designed HIT system can integrate a contract management system that automates the processes of reviewing the contract template, authorizing/approving the contract, storing it, managing different versions, renewal process reminders, and warnings of impending expirations.

## **THE STEPS TO MANAGING RISK AND COMPLIANCE**

Healthcare executives and providers can and should implement risk and compliance management from the very beginning of HIT development. One approach to risk and compliance management is following a two-phase, nine-step process (see Table 2). The first phase is *Assessment* (green steps) and the second phase is *Design and Implementation* (blue steps).

**Table 2: Steps in Managing Risk and Compliance**



Source: Frost & Sullivan

It is important to budget for and execute an assessment early enough to support MU achievement. Your organization's legal and regulatory professionals need to be included in the assessment phase and design and implementation phase in order to meet organizational, HITECH, HIPAA, and MU requirements. The assessment phase is likely an exercise needing a budget of mid-five figures and a timetable of four to five weeks to execute. The budget and timetable for the design and implementation phase will vary depending upon the specific needs of each organization, but organizations should expect a minimum of eight to 12 months from master plan development to initial implementation evaluation and adjustment.

The assessment phase needs to include outside organizations that may have access to patient information, such as medical transcription services, third-party billers and other financial support services, pharmaceutical companies and pharmacies, and life science organizations. Healthcare organizations need to educate their business associates regarding their requirements to meet standards associated with risk and compliance, and must update agreements to include the requirement to comply with HIPAA and HITECH. If the assessment determines that any business associate fails to meet these requirements, and is unable to comply, it is the responsibility of the healthcare organization to end their relationship with this outside organization or face penalties.

**Define sensitive information:** WHAT DATA NEEDS PROTECTING? WHO IS AUTHORIZED TO ACCESS THIS DATA? The first step in managing risk and compliance is defining what information is sensitive and who is allowed to access it. An organization may define information beyond protected health information (PHI), as defined by HIPAA, as

sensitive depending upon the data's role and the guidance of the organization's own legal and compliance staff.

**Discover and classify sensitive information:** WHERE IS THIS DATA? Sensitive information may be found in multiple locations—clinical workstations, billing offices, applications, networks, USB drives, EHRs, or paper files. Identifying and classifying it is critical to understanding a provider's risk and compliance needs and developing an appropriate plan, including necessary infrastructure.

**Map current information flow:** WHERE DOES THIS DATA FLOW? Understanding an organization's current flow of information provides the basis upon which risks are identified and risk management is designed. It also illuminates areas where better information sharing, improved efficiencies and cost-savings can be developed.

**Assess data breach and noncompliance risks:** WHO CAN ACCESS THIS DATA? Every time a node is added to a network, the risks of data breaches are magnified. For example, organizations need to consider the security of every medical device that connects into patient information systems.

**Assess opportunities to improve healthcare and improve costs:** HOW CAN THIS DATA IMPROVE HEALTHCARE AND LOWER COSTS? A HIT plan obviously has goals beyond risk and compliance management, and any good assessment will combine these concerns with the larger goals of improving healthcare and lowering costs. A good HIT system integrates all of these goals.

**Devise master plan:** HOW WILL THIS DATA BE SHARED AND PROTECTED? A master plan should include the definition of sensitive information, who may access it, who may change it, how changes will be tracked, audit and investigation plans, HIPAA-compliant technology to be used, ongoing maintenance and upgrade plans, testing and evaluation plans, certification plans, and budget and timeline.

**Implement master plan:** WHEN WILL THIS DATA BECOME ACCESSIBLE AND PROTECTED? The costs and timeline for establishing a HIT system will vary depending upon an organization's size and the complexity of its needs, such as the number and types of organizations with which it shares PHI. Small businesses focused on limited tasks, such as medical transcription, should plan for a minimum budget of \$3 million to \$5 million and 14 months, while the largest and most complex HIE might need to invest \$15 million to \$20 million or more and 24 months before they have a certified, fully functioning system.

**Evaluate, plan, and adjust as needed:** IS THIS DATA SECURE AND ARE WE COMPLIANT? An evaluation of both the *process* and *outcome* is critical. A *process evaluation* examines whether or not the project was implemented as planned and identifies any challenges encountered in implementation. An *outcome evaluation* examines whether or not the goals have been achieved. There are numerous reasons to do both: ensure future implementations run smoothly, ensure the plan is working and adjust it accordingly, identify staff who may need more training, and demonstrate to stakeholders the plan works.

**Continue evaluating, monitoring, and adapting as needed:** DOES THIS DATA CONTINUE TO BE SECURE AND DO WE REMAIN COMPLIANT? HIT risk and compliance management is a never-ending process. Policies, procedures, and infrastructure need regular evaluation to ensure they meet current needs and regulations and can accommodate current technology. For example, is a provider's storage capacity sufficient for the latest data-intensive medical devices? A well-designed master plan will minimize the need for upgrading HIT, but early adoption of advanced technology is more cost-efficient and secure than late, reactive adoption.

## EXAMPLES OF STRATEGIES FOR MANAGING RISK AND COMPLIANCE

There are numerous innovative strategies and technologies for managing risk and compliance. The most appropriate strategy for an organization will depend on several factors, including budget, complexity of data sharing needs, data storage needs, provider needs, and the patient populations being served.

Virtual desktops, where information is always housed in the network (not on a device's hard drive), can be accessed from any connected device via a secure login, providing greater security. Encapsulating information with metadata, ensuring that information cannot move unless it is going to a trusted zone of equal security strength, and having the ability to disable downloading of information all provide access to data without the risks associated with data stored on hard drives (e.g., lost unencrypted laptops or USB flash drives).

Dashboards, user interfaces that integrate information from several sources, are helpful in monitoring risks and compliance along with any other metrics, such as key performance indicators. Often designed to look like an automobile dashboard, IT dashboards provide graphical summaries of important data. And since they integrate information, they provide a holistic understanding of performance, so a hospital, for example, might want a dashboard to monitor key performance indicators and risks associated with those indicators or all measurements of HIPAA and HITECH compliance.<sup>10</sup>

## CONCLUSION

Clearly, risk and compliance management are a necessity in the development and implementation of HIT systems. Providers, business associates, and any organizations handling protected health information need to take the risks of breaches seriously. This is best done by working with qualified professionals to assess your organization's current risk and security situation, develop and implement a plan, and continuously evaluate and test your plan. The costs of planning ahead will always be less than not doing so.

---

<sup>10</sup> Wolan, J. 2010. "Use of Dashboards to Unify Performance, Risk and Compliance Management." <http://blog.idashboards.com/?p=213> (April 7, 2011)

## ACRONYMS AND DEFINITIONS

### **ACO**—Accountable Care Organization

Under PPACA, a network of doctors and hospitals that have agreed to provide all healthcare needs for a minimum of 5,000 Medicare patients.

### **CSF**—HITRUST Common Security Framework

“A framework that normalizes the security requirements of healthcare organizations, including federal (e.g., ARRA and HIPAA), state (Massachusetts), third party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS).”<sup>11</sup> The HITRUST CSF Assurance Program provides compliance assessment and reporting for HIPAA, HITECH, state, and business associate requirements.

### **EHR**—Electronic Health Record

“An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization.”<sup>12</sup>

### **EMR**—Electronic Medical Records

“An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one healthcare organization.”<sup>13</sup>

### **HIE**—Health Information Exchanges

“The electronic movement of health-related information among organizations according to nationally recognized standards.”<sup>14</sup>

### **HIT**—Health Information Technology

“The application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of healthcare information, data, and knowledge for communication and decision-making.”<sup>15</sup>

---

<sup>11</sup> <http://www.hitrustalliance.net/assurance/>

<sup>12</sup> NAHIT. 2008. Defining Key Health Information Technology Terms. Washington, D.C.: Department of Health and Human Services.

<sup>13</sup> *Ibid.*

<sup>14</sup> *Ibid.*

<sup>15</sup> Brailer, D. and T. Thompson. 2004. Health IT Strategic Framework. Washington, D.C.: Department of Health and Human Services.

## **HITECH**—Health Information Technology for Economic and Clinical Health Act

As part of the American Recovery and Reinvestment Act (ARRA) of 2009, it provides incentives for the adoption of electronic health record systems among providers and enhances privacy and security measures under HIPAA.

## **HITRUST**—Health Information Trust Alliance

A private, independent company working in collaboration with healthcare, business, technology, and information security leaders to make information security a core pillar of health information systems and exchanges.

## **MU**—Meaningful Use

Refers to the requirement in the HITECH Act that EHR systems are used in a meaningful way. ARRA defines Meaningful Use as consisting of: use of certified EHR in a meaningful manner; use of certified EHR technology for electronic exchange of health information to improve quality of healthcare; use of certified EHR technology to submit clinical quality and other measures.

## **PCMH**—Patient-Centered Medical Home

“A Patient-Centered Medical Home is a team-based model of care led by a personal physician who provides continuous and coordinated care throughout a patient's lifetime to maximize health outcomes. The PCMH practice is responsible for providing for all of a patient's healthcare needs or appropriately arranging care with other qualified professionals. This includes the provision of preventive services, treatment of acute and chronic illness, and assistance with end-of-life issues. It is a model of practice in which a team of health professionals, coordinated by a personal physician, works collaboratively to provide high levels of care, access and communication, care coordination and integration, and care quality and safety.”<sup>16</sup>

## **PHI**—Protected Health Information

Individually identifiable health information relating to a person's physical or mental health, healthcare he or she has received, payment for healthcare, demographic data, or identifiers such as name, address, date of birth, or Social Security Number.

## **PHR**—Personal Health Record

“An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.”<sup>17</sup>

---

<sup>16</sup> American College of Physicians. 2011. “What is the Patient-Centered Medical Home?” [http://www.acponline.org/running\\_practice/pcmh/understanding/what.htm](http://www.acponline.org/running_practice/pcmh/understanding/what.htm) (April 5, 2011)

<sup>17</sup> NAHIT. 2008. Defining Key Health Information Technology Terms. Washington, D.C.: Department of Health and Human Services.

## CONTACT US

Auckland  
Bangkok  
Beijing  
Bengaluru  
Bogotá  
Buenos Aires  
Cape Town  
Chennai  
Colombo  
Delhi / NCR  
Dhaka  
Dubai  
Frankfurt  
Hong Kong  
Istanbul  
Jakarta  
Kolkata  
Kuala Lumpur  
London  
Mexico City  
Milan  
Moscow  
Mumbai  
Manhattan  
Oxford  
Paris  
Rockville Centre  
San Antonio  
São Paulo  
Seoul  
Shanghai  
Silicon Valley  
Singapore  
Sophia Antipolis  
Sydney  
Taipei  
Tel Aviv  
Tokyo  
Toronto  
Warsaw

**Silicon Valley**  
331 E. Evelyn Ave. Suite 100  
Mountain View, CA 94041  
Tel 650.475.4500  
Fax 650.475.1570

**San Antonio**  
7550 West Interstate 10, Suite 400,  
San Antonio, Texas 78229-5616  
Tel 210.348.1000  
Fax 210.348.1003

**London**  
4, Grosvenor Gardens,  
London SW1W 0DH, UK  
Tel 44(0)20 7730 3438  
Fax 44(0)20 7730 3343

**877.GoFrost**  
[myfrost@frost.com](mailto:myfrost@frost.com)  
<http://www.frost.com>

### ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.

For information regarding permission, write:

Frost & Sullivan  
331 E. Evelyn Ave. Suite 100  
Mountain View, CA 94041