CURRENT PERSPECTIVES ON MANAGING RISK AND COMPLIANCE IN HEALTHCARE:

THE NEED FOR TRUSTED HEALTHCARE INFORMATION
In January 2011, CDW Healthcare surveyed 1,000 adults from the U.S. who had been to a physician’s office, a hospital, or an outpatient facility in the past 18 months. The survey revealed that a number of respondents were uneasy about potential security problems associated with the move from paper to electronic health records. Nearly half of all respondents believed that using electronic health records would negatively impact the privacy of their personal information and health data. Patients’ concerns varied from fears that their information would end up on the Internet, to cybercriminals using the information to steal their identity. Survey respondents also worried that if employers gained access to their health information, they could potentially use it to manage their benefits and compensation, or to make hiring decisions.

Regardless of whether a healthcare organization is just beginning to implement an Electronic Health Record (EHR), or transforming electronic care processes for accelerated service delivery, an important consideration for using and maintaining electronic healthcare information meaningfully is mitigating the potential risk to those records, and managing compliance to relevant regulatory requirements. The pressure is coming from several different directions. The increasing use of Personal Health Information (PHI) and patient portals are stoking security concerns. Healthcare consumers are knowledgeable and demand privacy and trust protections for their data. Just as in other businesses, healthcare consumers want safeguards against medical identity theft and fraud.

HOW RISK IS DEFINED IN HEALTHCARE

The Health Insurance Portability and Accountability Act’s (HIPAA) Privacy Rule requires health plans, healthcare clearinghouses, and most healthcare providers (covered entities) to protect the privacy of patient information through administrative, physical, and technical safeguards at all times. Prominently included in a healthcare organization’s HIPAA or HITECH (The American Recovery and Reinvestment Act of 2009’s component: the Health Information Technology for Economic and Clinical Health Act) compliance plans should be a risk analysis that would account for how various systems that generate regulated electronic health records could potentially affect the safety of the patient.

Although there are many definitions of “risk” depending on your industry and perspective, a useful one comes from the ISO/IEC Guide 51:1999. Risk is “a combination of the probability of occurrence of harm, and the severity of that harm.” Whether applied to HITECH, HIPAA, the EU Data Directives, or The Joint Commission’s Information Management Standard, the regulatory perspective for risk should focus on risk to healthcare quality and/or public safety, as in when a computerized system generates or stores electronic health records that can greatly impact healthcare safety and quality.

In addition, regarding patient clinical compliance challenges, there are also regulatory issues from an operational perspective—not only for provider organizations, but also for payers. Identified risks may be addressed by technical fixes that effectively eliminate the risks, reduce the likelihood of occurrence, or the severity of consequences to acceptable levels. Risks for which there are no technical fixes may perhaps be addressed by procedural adjustments. Other residual risks following mitigation may be perceived as minimal and within acceptable risk levels.

The Joint Commission and HIPAA require healthcare organizations to demonstrate that policies and procedures are easily accessible while meeting security and privacy requirements. Despite this, many hospitals, laboratories, and pharmacies continue to maintain manually-driven systems where document-based policies and standard operating procedures (SOPs), sometimes in paper form, require special intervention to create, update, retrieve, and
This manual approach to policy and procedure management not only adversely impacts patient safety and privacy, but it also risks the organization’s accreditation, regulatory compliance, and overall operational effectiveness. Although the Joint Commission is U.S. focused, compliance policy-based management is an issue worldwide.

In addition, many of today’s healthcare contracts are not managed with an integrated enterprise approach but are instead handled with disparate point solutions and siloed departmental applications. As a result, contracts are stored in multiple locations with different retention schedules. Reporting across these varied repositories, and with a consolidated view, is almost impossible. This ineffective contract management system leads to risks and adverse outcomes; potential exposure is in the millions of dollars. In a recent news article, a U.S. hospital may have to pay a substantial sum for lapsed contracts related to referrals in violation of the Stark Law, where lapsed contracts that were not re-signed could cost a hospital in excess of $854,000 USD.

WHAT IS RISK MANAGEMENT?

Many healthcare organizations know what has to be done. They know that they must have a structure in place that clearly outlines data governance, business requirements, and the technology infrastructure and processes required to support a safe and secure computing environment. However, these same organizations are also faced with challenges that include a lack of funding for security initiatives, increasing regulatory requirements and standards, and the growing need to share data with the patient, partners, and collaborators. Add to this the fact that in many organizations, individuals, and departments have undertaken their own information technology initiatives—whether server-based applications or simple spreadsheets and databases—and it is easy to see how difficult the job of managing and protecting all of these data and process silos can be.

Regulatory agencies in the major world markets (the European Union, North America, Canada, and Japan) all strongly encourage the use of risk management protocols. They may not unequivocally express an explicit regulatory requirement for risk management or dictate exactly how to assess and manage risk, but the outcome of an overall comprehensive risk management protocol is encouraged by almost all regional laws and regulations for healthcare providers, payers, and government healthcare agencies.

Risk analysis should be a living, evolving process throughout the lifecycle of patient care or operational processes. The generic steps of a risk analysis protocol are to:

- Identify the potential hazards using cross-functional teams that might include engineering, R&D, clinicians, marketing, users, regulatory, product safety engineers, manufacturing, etc.
- Define the probability and risk of each hazard using either a bottom-up Failure Mode and Effect Analysis (FMEA) or a top-down Fault Tree Analysis (FTA)
- Determine which hazards have risk levels that require mitigation
- Mitigate the hazards
- Check to ensure no new hazards are generated
- Continue to mitigate hazards until the risk level is low enough to be acceptable

Another best practice for controlling risk in healthcare organizations is to establish a corrective and preventive action (CAPA) plan, and analyze and follow up on complaints during the healthcare record lifecycle.

When conducting a risk analysis, healthcare organizations are expected to identify possible hazards associated with their healthcare practices and relevant electronic systems, under both normal and fault conditions. The risks associated with those hazards, including those
resulting from human error, must then be calculated based on normal and fault conditions. If any risk is deemed unacceptable, it must be reduced to acceptable levels by the appropriate means, for example, by redesigning compliance policies or warnings.

An important part of risk analysis is ensuring that changes made to eliminate or minimize hazards do not introduce new hazards. Whereas healthcare organizations routinely manage a wide range of risks, external legal and regulatory compliance risks are arguably the key issue in e-Governance, Risk, and Compliance (eGRC).

**eGRC STRATEGIES FOR TRUSTED HEALTHCARE INFORMATION**

eGRC is an umbrella term that describes how an organization:

- Defines the objectives, policies, procedures, and standards by which it is managed
- Makes informed decisions to seize opportunities while avoiding or managing negative events and processes
- Demonstrates adherence to laws, regulations, policies, contractual obligations, and industry standards

eGRC is a combined area of focus in many healthcare organizations. The eGRC strategy is of immense importance to global healthcare organizations in both the private and public sectors. It has consistently registered as one of the major drivers for information security investment for many years.

With leading healthcare organizations adopting more mature eGRC processes, and integrating their eGRC systems more closely with their business systems, it is now an appropriate time to review how far enterprises have come and determine their future priorities. There is heartening evidence that eGRC processes are maturing. One problem with compliance as it is practiced today is that it is mostly based on periodic inspections. Organizations tend to drift out of compliance with regulations such as HIPAA, Joint Commission, and EU Data Directives between audits due to their evolution. As a result, there is a growing intention to integrate continuous controls monitoring into eGRC processes. However, eGRC faces new challenges as emerging IT technologies such as virtualization and the adoption of cloud services raise new issues relating to information integrity. The user community is still uncertain about what these issues are, and about their relative importance.

**REGULATION COMPLIANCE, COMPREHENSIVE PATIENT INFORMATION, EDUCATION, AND POLICIES AND PROCEDURES SIGHTED AS MAJOR CONCERNS**

During a recent conference on healthcare information systems management, EMC® surveyed attendees regarding their risk and compliance management concerns. Although there were some commonly expressed concerns from healthcare professionals (see sidebar), the healthcare CIOs, Project Directors, Trainers, Compliance Officers, and IT Directors surveyed conveyed differing opinions on what the biggest risks to their EHR environments were, and what to do about them.

A CIO from a non-profit healthcare provider in rural Arkansas explained that internal security is the biggest risk that they face for their EHR. He also said that: “Making sure that everybody understands the different federal regulations and that we remain compliant with things like HIPAA and HITECH” are also key challenges.

A director of Clinical Decision Support at a Children’s Hospital in Florida said: “On the clinical side, the biggest risk is that we’re still in a state where our record’s medium is fragmented. Not all of the patient information is in electronic form yet. This means that there is significant risk when a clinician is viewing a patient record that he may not see all of the
relevant patient information. This might lead to a higher risk for clinical errors, prescription/medication errors, errors of omission, and errors of commission.”

Several individuals stated that their biggest EHR risk is inappropriate access. One VP/CIO at a healthcare partnership in Colorado said that it was internal, rather than external, unauthorized access to patient information that posed the biggest risk: “Inappropriate access to patient records is more likely from internal sources rather than external sources. We are fairly confident in our perimeter defenses, but when someone is giving away an internal password or there is some other kind of internal breach, those are the things that we are having the hardest time managing.”

Training came up during these interviews as being paramount in helping to manage EHR risk and compliance. An IT director at a hospital in Colorado mentioned that: “Making sure that the employees follow the rules for securely working with electronic records is very important. We do extensive and frequent training for that.” Not only is training related to working with the EHR significant, but it is also important to educate on the proper process for interfacing with it.

The IT director added: “The biggest challenge is getting the security officers to understand that the need for portability has to be taken into consideration along with security. I try to get both sides—the clinicians and the information security officers—to understand that there is going to be both risk and reward in all that you do when using an EHR.”

A clinical workflow analyst for the U.S. military who works with the DoD’s EHR mentioned that it was very important to make sure that you train exactly to your policies to ensure low risk as well as compliance with regulations. A VP of Operations said that including his clinicians in the development and testing of their EHR is the key to getting them to understand where risks may reside: “Make sure that they are part of developing the requirements. Make sure that they are part of the iterative steps of program development and testing. We get physicians from the field to come in sit down, work through the EHR as we test it—we do what’s called unit testing, and work through that. We make sure that they are accepting of the product before they start using it.”

Putting a formal risk assessment process in place, as was mentioned in a previous section of this paper, was brought up often by the respondents of the EMC survey. The VP of Operations at a healthcare consultancy said: “Our job is to try to identify the risk, mitigate the risk, and then find out what the risk controls are: i.e. is it additional funding; is it an extended timeline; is it acceptance of risk? We are also trying to quantify the risk so that we can then put the appropriate mitigations in place.”

He also remarked: “We do a formal risk assessment; we look at the probability of occurrence, the impact of the risk, and severity of the risk. Basically, we have a dashboard that we put together to track risks, and we brief it to the customers every month or so on a regular basis as we work to mitigate those risks.”

A Project Manager for a Health Information Technology Regional Extension Center for Nebraska stated: “Performing a risk assessment for EHR use is part of what it means to become an EHR meaningful user.” A healthcare CIO in Nashville, TN reported doing a Gap Analysis against ARRA’s Meaningful Use requirements rather than a more formal risk assessment.

Another significant challenge for these users is the proper interpretation of healthcare regulations. Keeping current with any changes or amendments to the regulations is also critical for managing risk and compliance for the EHR. When asked how to get consistent and accurate interpretation of the regulations, the military clinical workflow analyst stated: “Just verify and ask more questions. If we’re not sure, we ask for more clarification. In working in a facility that’s a military treatment facility, we know those in the right places and ask the right questions to ensure that we’re doing the right thing.”
“We have a legal partner who helps us if true legal advice in interpreting regulations is needed. When it comes to interpreting ARRA, and meaningful use guidelines, we give them our recommendations based on what we know. I am our “meaningful use expert”, said an IT director from Addison, TX.

To communicate a company-wide interpretation of the healthcare regulations, and to help the EHR stakeholders in an organization understand that interpretation, a clinical engineer in Little Rock, AR, uses conference calls, meetings, and internal messages: “We bring the security officers to the clinicians, we educate the clinicians on the need for security, and we talk to them about the protocols that are required. We try to get both sides to understand the perspective of each other.”

Another IT director, who is part of an IT peer group that discusses healthcare regulation interpretation, offered information about it: “There is a Western HC Alliance Group, and all of the IT Directors meet every three months, as well as every month on webcam. We have speakers and we try and keep up to date. If somebody finds something out, they spread the word—we have a little community.”

MOBILE DEVICES REQUIRE CRITICAL ATTENTION TO RISK AND COMPLIANCE

EMC next asked about how the use of mobile devices affects the security and privacy of electronic patient data. Nearly all of the survey respondents mentioned that they use mobile devices in a clinical setting to better serve patients, but that use of these devices requires critical attention to risk and compliance.

An IT manager from a Florida hospital said: “There are a lot of security risks with mobile devices so you have to look at a means of secure access through dedicated lines or dedicated channels, in combination with encryption methodologies.”

A VP of Operations in Washington, DC, had an interesting take on the security of mobile devices: “Remember that the device is just a plane for information—that’s all it is. People get tied up in the devices, but you shouldn’t; you need to be focused on your patient data. If you are focused on the data, you’re going to use that information as one of your tools to treat that patient—just like your stethoscope.” In essence, what’s important is protecting the data wherever it lives, rather than just focusing on the mobile device.

The owner of a consultancy in North Carolina disagrees: “Obviously no data should be stored on the mobile device, but you never know what gets cached, so you have to be very careful about that.”

The CIO from Nashville reiterated the concern for the security of mobile devices: “I believe that mobile devices pose the biggest risk because our procedures inside our clinics are pretty guarded. We’ve got physical security there. It is the mobile devices—or access from outside the system—that poses the greatest risk.”

BUSINESS RISKS ARE A COST ISSUE

The last topic for query during the EMC survey was regarding business risks related to the use of EHR in general. The business risks identified by our survey respondents were; cost of implementing and maintaining an EHR; staying on timelines and delivering the organization’s product or service; maintaining a cost-to-schedule performance ratio; relying on an EHR vendor for risk and compliance controls, and fear of the unknown when implementing or upgrading a new EHR.

A Compliance Officer and Clinician from Palmetto, FL said: “For a solo practitioner like me, “cost is the biggest risk. HITECH is great if you are an IDN or a hospital, but we’re not
considered an eligible professional under HITECH funding. However, we’re still expected to be interoperable.”

“When customizing an EHR, the risk is not from any breached access point, it’s more on the management side. Small updates and changes lead to a business continuity risk,” mentioned the CIO from Colorado.

A Health IT Projects Leader from Louisiana said: “What I’m seeing as a risk is fear of how using the EHR is going to change the clinician’s workflow and their practice. They are afraid that it’s going to add more burdens, so they develop inertia.”

**EMC BUILDS A TRUSTED HEALTHCARE ENVIRONMENT**

EMC is able to provide key solutions for healthcare organizations struggling with managing risk and compliance. EMC combines an understanding of the clinical, operational, and business requirements for information technology management in healthcare organizations with knowledge of the regulatory requirements facing them. EMC then leverages that understanding and knowledge, along with technical and process expertise, to enable these entities to manage and operate a secure and compliant technology environment.

EMC’s comprehensive assessment of an organization’s security posture follows the Common Security Framework (CSF) of the Health Information Trust (HITRUST) Alliance, incorporating standards applicable to healthcare organizations and their business associates. This includes HIPAA, HITECH, EU Data Directives, PCI Data Security Standards, and Information Management requirements of the Joint Commission, as well as U.S. state-specific regulatory requirements.

EMC Information Risk Management Solutions for Protected Health Information are based on global industry standards and best practices, such as ISO 27002 and ISO 27799 for Health Informatics, to meet the compliance requirements of healthcare organizations of all sizes.

**EMC’s Trust Framework**

![EMC’s Trust Framework for Managing Information Infrastructure Risk and Compliance](image)

Figure 1. EMC’s Trust Framework for Managing Information Infrastructure Risk and Compliance
The EMC Virtual Desktop Solution for Healthcare improves clinical workflows and patient safety by providing immediately accessible, always available desktops that follow clinicians wherever they go. EMC Infrastructure and VMware® View™ enable clinicians to access all applications and patient data from any device and from any location with a consistent, high-quality user experience. Client images and patient data stay in the data center and are managed centrally for strong security and compliance. Integration with Imprivata provides secure tap-and-go login, log-out and authentication with single sign on (SSO). Integration with RSA®, the security division of EMC, provides strong data protection and security/compliance monitoring. With EMC infrastructure and VMware View, data visibility is improved and management is automated from the desktop to the data center. Provisioning, patches, and updates are simplified and centralized to reduce costs and improve IT responsiveness.

EMC Consulting professionals and Proven Solutions for Healthcare let you deploy virtual desktops cost-effectively and with confidence to achieve desired results, both clinically and financially. EMC provides end-to-end expertise, including OS and applications, security and management, and virtualization. All services, including desktop virtualization assessments and business justifications, take into account the unique requirements of healthcare providers. EMC Proven Solutions and EMC Consulting professionals for healthcare ensure quick, low-risk implementation of any EMC product for healthcare.

EMC is also the leading provider of disk-based backup and recovery solutions, and leads the industry in deduplication storage and software. EMC’s portfolio of backup and recovery products provide the flexibility and scalability to meet the data protection needs of healthcare enterprises of all sizes.

EMC Information Intelligence helps healthcare organizations become more agile, responsive, and competitive by enabling them to get the most out of their information. It ensures that information is accessible and properly managed, stored, and secured. When intelligence is built into the information infrastructure, the right information is always available when and where it’s needed. With information intelligence, healthcare organizations can make the right decisions while reducing cost and risk. Also, with solutions developed by EMC’s world-class partners, the opportunities to leverage information intelligence throughout a healthcare organization are virtually unlimited. Information intelligence can exploit the natural relationships between content and processes that exist in areas such as hospital admissions, patient care delivery, benefits administration, claims processing, and customer service.

In addition, EMC’s Policy Management of Information Solutions afford end-to-end content and processing for creating, updating, storing, and searching for healthcare documents. This is accomplished by automating and streamlining their lifecycle through workflows and business rules. EMC’s Policy Management of Information Solutions also provide dashboards and reporting functionality to supply end users with knowledge about where the latest documents are and ensure that policies and procedures are easily accessible—all while meeting security and privacy requirements.

EMC’s Policy Management of Information Solutions are designed to minimize risk, control costs, and reduce cost of ownership by delivering the benefit of centralized, online document and records management—even for legal contracts. Legal contracts management delivers end-to-end content and process solutions for creating, updating, storing, reporting, and searching for contracts. It can be used, for example, to produce a current, valid document requested by the Joint Commission during a survey.
CONCLUSION

To preserve patients' safety and protect their information, the key is to reduce information management risks down to their lowest possible levels, and prove adherence to healthcare regulations. Implementing and maintaining a secure and compliant IT infrastructure for patient information is a critical part of the risk mitigation process. It is also important to implement and maintain a solid risk assessment and management policy.

Choosing an experienced IT infrastructure organization with the right tools and expertise in managing risk and compliance in the healthcare arena is paramount. EMC's healthcare solutions enable healthcare organizations to simply and efficiently use information to make more informed clinical, operational, and financial decisions while managing risk and compliance in a cost effective manner.