White Paper

Risks Associated with Missing Documentation for Health Care Providers

Well-Documented Controls Reduce Risk and Support Compliance Initiatives
Many Health Care Organizations Lack Well-Documented Controls or Processes

Health care organizations are challenged to protect patient data and comply with regulations governing health care entities. Having well-documented policies and controls is an important part of reducing risk and achieving compliance. This paper discusses the need for well-documented controls to reduce risk, along with expert suggestions for improving documentation.

The absence of well-documented controls leads to gaps in security risk control processes. This creates a security environment that is difficult to monitor or measure and can lead to non compliance with Health Insurance Portability and Accountability Act (HIPAA) requirements and extensive fines.

Some areas that are frequently found to be be deficient during HIPAA gap or compliance reviews include annual and ongoing risk assessments, undocumented policies and controls and unwritten processes or procedures. The descriptions below define examples of some common findings Solutionary has uncovered while conducting these assessments.

- **Risk Assessment** – Organizations typically have tried to create controls without properly identifying the risks which define the controls. A proper risk assessment will highlight areas that are in need of monitoring, controls which need to be defined and a way to measure and monitor the controls to ensure the controls are operating as designed. A properly executed risk assessment will address risks of loss and exposure of protected health information (PHI) as well as supporting clinical and non clinical systems. Quantifying the risk, giving the risk a priority ranking and then documenting the risk gives the organization a starting point to identify the required controls.
• **Policies and Controls** – Policies are the overarching documentation which sets the position and tone of the organization’s control posture. Controls are written and established by an organization to verify a regulatory requirement or risk is properly addressed and monitored. Health care organizations often address controls in “silos” or by specific departments in the organization, not looking at the whole picture. For example, the outpatient clinic may have a set of controls in place to monitor access to patient information, but the controls are different from the patient information controls used at the admissions office for the hospital. Why isn’t there a unified set of controls for all areas that handle patient information? A disjointed approach often leads to duplicate controls, an environment which is not easily monitored and the inability to determine if the controls are operating effectively.

• **Processes or Procedures** – Processes and procedures are the activities that support documented controls and enforce policies or standards. These documented controls then provide measures and checks to support the policies or standards in place. Processes and procedures are usually repetitive and, based on experience, are not well documented. Unfortunately, even if a health care organization has controls in place, lack of proper documentation can still lead to an audit finding for noncompliance.

  For example: Joan works at the help desk. Every day, Joan comes into work, logs into the network and checks her email for trouble tickets. She responds to the tickets based on her experience and sends them to the proper group for remediation or repair. Joan repeats this process daily, as well as everyone else who works the help desk. Everyone on the help desk is familiar with the process flow and where to send trouble tickets; however the process for logging in, groups or persons to be notified, logging tickets and closing out tickets, is not documented, and is, therefore, not truly HIPAA compliant.

In the example above, there are a lot of problems that may not be obvious to an organization. Some of the areas of concern are common and often overlooked. Some of the questions an assessor might ask to help the organization define and fix the identified gaps are listed below:

- What groups are supposed to receive the trouble tickets?
- How does the help desk verify the jobs are closed out?
- What is the data flow for trouble tickets?
- How does an assessor or internal auditor measure the effectiveness of the help desk without documented processes to verify the controls are in place?

Properly identifying risks and then documenting the risks, controls and processes or procedures creates a measurable environment which can be assessed to determine if there are gaps or areas which can be improved.
The assessor can verify the processes supporting the controls around the help desk are in place by observing the help desk personnel, but how does the assessor provide proof without documented controls and processes or procedures? Properly identifying risks and then documenting the risks, controls and processes or procedures creates a measurable environment which can be assessed to determine if there are gaps or areas which can be improved.

At an Office of Civil Rights (OCR) and National Institute of Standards and Technology (NIST) conference, OCR conducted a presentation on the initial results of the HIPAA privacy and security audits. The biggest privacy findings included the lack of policies and procedures. Non-compliance with Administrative Safeguards requirements within the HIPAA Security Rule accounted for 42% of the audit findings, of which, some of the biggest issues noted involved the absence of risk assessments.

**Questions to consider when reviewing documented controls or procedures to understand if they are in place:**

- Has a proper risk assessment been completed to determine if areas needing documented controls have those controls in place?
- Do the controls have properly documented processes and procedures in place to monitor controls in the environment?
- Does the control structure have an overarching security or risk policy to ensure all controls have been defined?
- Does the organization understand all of the areas which need to have documentation to mitigate their risk when handling ePHI?
- Does the documentation support the identified areas of risk?
Documentation to Maintain Compliance

Maintaining compliance is a process. Processes need to be recorded in documents. No documents equals no compliance equals increased risk. Good documentation consists of processes, recurring procedures and a set of controls that mitigate identified risks and protect system security and patient information.
About Solutionary Security Consulting Services

Solutionary Security Consulting Services (SCS) specializes in the delivery of independent security guidance, security controls validation, standards-based compliance and remediation design and support. SCS consultants engage in recurring, scheduled security and compliance initiatives or short-term, one-time projects; whichever best meets the needs of the organization. SCS Offensive Security Services include technical security testing like Penetration Testing and Application Security Assessments as well as Physical Security Assessments and Social Engineering Assessments. Governance Risk and Compliance services include Vendor Risk Management and Risk Methodology as well as services to support compliance with security frameworks and mandates like the Payment Card Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), HIPAA/HITECH and others.

Solutionary is a trusted consulting leader in the health care industry with demonstrable understanding of the entire health care value chain. Solutionary is an expert in protecting data while also enabling health care organizations to fulfill their mission — to save lives.

SCS Services for Health Care Include:

- HIPAA Assessment (including HITECH and Omnibus)
  - HIPAA Readiness Assessment
  - HIPAA Compliance Attestation
  - Meaningful Use Attestation

- HITRUST Assessment
  - HITRUST Assessment – Validated Report
  - HITRUST Assessment – Certified Report
  - Yearly Risk Assessment (Non-certification years)
  - MyCSF Population Assistance (HITRUST GRC tool)

- Security Practices
  - Third Party Assessments
  - Risk Assessment Methodology
About Solutionary

Solutionary, an NTT Group security company (NYSE: NTT), is the next generation managed security service provider (MSSP), focused on delivering managed security services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients’ internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

For more information, visit www.solutionary.com

Learn More

To learn more about security consulting services and to meet your compliance needs, contact Solutionary today at SCSManagement@solutionary.com

ActiveGuard® US Patent Numbers: 7,168,093; 7,424,743; 6,988,208; 7,370,359; 7,673,049; 7,954,159; 8,261,347.

Solutionary, the Solutionary logo, ActiveGuard, the ActiveGuard logo, are registered trademarks or service marks of Solutionary, Inc. in the United States. Other marks and brands may be claimed as the property of others. The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright ©2014 Solutionary, Inc.