



Information Risk Assessment Program for Healthcare Data Protection

The Risk Assessment Program provides a valuable service that helps identify your user and information activities that are subject to data leakage and privacy risk. The program will help your organization start to identify information access and use patterns, apply proper controls, and prevent HIPAA or company policy violations.

Information Risk Management

Reducing information misuse and improper disclosure is a major concern for today's hospitals and health insurers. Monitoring and controlling information entitlement rights to identify and mitigate risk is an imperative for data security and compliance. Rapid, dynamic implementation of information control procedures is essential to remain protected. Now, hospitals and health insurers are more exposed due to increased connectivity, workforce mobility, and dependence on a caregiver ecosystem consisting of remote practices, partners, and suppliers.

Managing information risk, achieving compliance with HIPAA regulations and company best practices, and protecting patient and financial data from leakage and privacy violations are challenging within dynamic, complex information networks. Protecting data, training the staff to act responsibly, and demonstrating control of information can be costly and time-consuming. Organization leaders strive not only to meet compliance and control risk, but also to achieve greater effectiveness and productivity.

Why is Managing My Information Risks Difficult?

Managing healthcare data leakage and privacy risk begins with a factual assessment of where healthcare data is; how it is being accessed; what conditions are creating risk. Yet discovering and identifying this baseline data, especially during the time access is attempted, can be extremely difficult.

For example, nurses with access to patient records may be able to copy diagnostic codes into public documents. Similarly, a patient's health insurance financial data can be disclosed over email to unauthorized recipients or without following best practices to apply encryption.

To avoid risks, policies must be able to evaluate the real-time business conditions during healthcare data access and handling. Factors such as file attributes; user or group role; locations of data, user, or connecting devices; time of access or use; and similar conditions can determine exposure when information handling occurs.

The Information Risk Assessment Program

The program addresses the difficulties associated with discovering and identifying healthcare data access and use activities. This insight is necessary to help you develop and strengthen your efforts in managing data leakage and privacy risk. You can learn who currently owns or has access to healthcare data, how to ensure proper information control policy, and where leakage or privacy violation activities are occurring.

What Does the Program Do?

You are provided a "snapshot" of user and information activities. This includes the access and handling of healthcare data, inside and outside your organization, on or off your network. You will receive baseline data that helps you discover the level of risk of improper information access and handling that can result in leakage or privacy violations. You can uncover deficiencies or gaps in current security practices to improve and automate compliance and audits. Our findings and recommendations will help you:

- **Educate users on proper ways to access and handle healthcare data:** Discover areas to focus or improve policy training. Improved education helps users to access and handle healthcare data in a manner that is compliant with your policies and HIPAA.
- **Automate information security rules, and data access and handling procedures:** Obtain insight into the volume and types of healthcare data, or sensitive, confidential data, that are vulnerable to leakage or privacy violations on your organization's network. Automating procedures can improve efficiency, and reduce complexity and errors.
- **Identify or discover policy gaps:** Gain awareness into potential non-compliance due to unintentionally risky or undefined procedures. Such gaps may include data disclosed, or user access rights assigned, improperly. Simplifying or optimizing security rules or procedures can close these gaps, and improve policy effectiveness and manageability.

What Will I Receive from the Program?

You will receive concise facts focused at user and information access and handling activities at data servers, portals, and endpoints (e.g., Windows file servers, Microsoft® SharePoint, Linux file servers, Windows PCs and laptops), along with our analysis and recommendations.

Our discoveries, analysis, and recommendations are delivered in a presentation and an *Executive Healthcare Information Risk Assessment Report*. The report provides an extensive view containing:

- **Information Access, Use and Disclosure Patterns:** Healthcare data access and handling by user, time of access and use, access location by user or data, and proportion of access and use outside business hours, and remote access and use. Activities can include:
 - When and how different users, groups, departments, or organizations share healthcare data.
 - Which users or groups access or use data disproportionately outside of normal work hours.
 - What information is accessed or used by users or systems that are outside of internal domains.
 - What data is communicated to points outside the network or copied to removable media (e.g., USB).
 - What systems are used to share healthcare data.
- **Overprivileged Users:** Many IT organizations grant access privileges to more users than required, creating unknown risks. This report details:
 - Which authorized users and groups have access rights, but have *not* accessed healthcare information, on file servers or SharePoint servers.

Report findings can then be used to limit access only to appropriate users with rights to access or use data.

- **Control Point Summary:** Activities summary for specific applications, endpoints, or data repositories (e.g., patient records application or server, SharePoint, laptops, Outlook email clients). Activities can include:
 - What healthcare data was attempted to be accessed on a system or shared using an application.
 - What data is accessed or shared based on group role.
 - Which users have accessed or shared specific files.
 - What healthcare data is accessed or shared most.
 - Which users access or share the most information.

Our findings will identify areas of risk and recommendations for rapid remediation when necessary.

How Do We Engage?

The program engagement process is designed to be convenient for you and transparent for your organization, making it easy to achieve fast results. Minimal client-side software installation is needed in your user environment.

Once you contact us, one of our Information Risk Professionals will respond to answer your questions and provide you with a questionnaire:

1. You complete a simple questionnaire that we provide.
2. Using the information you provided in the questionnaire, we will conduct a brief discovery session with you to establish success criteria for the assessment exercise. This will include, as applicable:
 - a. Identify a set of healthcare information locations, sites, and applications. We may need an LDIF export from Microsoft® Active Directory®.
 - b. Identify a set of applications, endpoints, and servers that you will conduct the information risk assessment upon. We may need access where an agent can be automatically installed.
3. We will quickly configure and deploy the necessary software to perform the discovery. User and information activity data will be collected unobtrusively, based upon the requirements you have provided.
4. After a period of data collection, we will synthesize and provide you with the results and our analysis in a Risk Assessment presentation and *Executive Healthcare Information Risk Assessment Report*.

Time Requirements: Depending on the computing environment and success criteria, the program can take as little as one week.

Confidentiality and Privacy Assured

All data collected is aggregated at our servers, hosted at a secured facility. All information and results from our analysis are held in strictest confidence and removed from our systems, post-engagement.

Get Started by Contacting NextLabs

For More Information about our Information Risk Assessment Program for Healthcare Data Protection:

- Call NextLabs today at **650-577-9101**
- Visit us on the Web at **www.nextlabs.com**