Solution Brief

Healthcare Data Protection

Protect Patient & Subscriber Data Across Hospitals, Insurers, and Ancillary Providers By Monitoring Disclosure, Educating Users About Policies, Automating Safe Handling Procedures, and Preventing Misuse

OVERVIEW

Healthcare information, including patient medical records and health insurance subscriber data, is accessed and used today within a complex ecosystem of hospitals, insurers, and ancillary service providers. With multiple organizations allowing discretionary access to this data across departments and teams, the potential risk of improper disclosure is high. And when healthcare data is leaked, organizations have difficulties maintaining their reputation and customer loyalty, in addition to devastating HIPAA fines and remediation expenses.

Today's basic access controls do not adequately discriminate the user roles and business conditions that determine proper rights to access and handle data. Moreover, after access is granted, an authorized user can freely distribute healthcare data on public networks, send it externally via e-mail or instant message, or leave records unattended. It is unrealistic to manually educate users to always follow complex procedures to protect data. Management overhead, lack of coordination and user education, and human error all increase the risks of violating policies and procedures.

SOLUTION HIGHLIGHTS

- Discover how data is accessed and handled to identify gaps in protection
- Educate users about the proper ways to handle data to comply with HIPAA policies and procedures
- Automate healthcare data distribution procedures to prevent leaks and optimize business results
- Reduce fines and remediationexpenses by managing disclosure to authorized users and teams
- Prevent misuse that compromises business integrity, reputation, and customer loyalty
- Investigate misuse and demonstrate policy effectiveness, inside and outside the organization

THE SOLUTION

Active Control for Healthcare Data Protection ensures proper access, handling, and disclosure of patient records and health insurance subscriber data. The solution applies HIPAA and best practice policies by using controls deployed across applications and data repositories where healthare data is accessed and stored, and endpoints where it is handled and disclosed.

The solution optimizes a single, centrally-managed policy set and targets it across different platforms, applications, locations, and data types. Universal controls are enforced across heterogeneous applications and systems, such as healthcare IT systems and PC desktops, to preserve data integrity throughout its entire lifecycle.

Healthcare organizations can now unify healthcare data access entitlements and handling policy. The solution educates users about policies and procedures, automates procedures when organizations collaborate and use data, and protects against improper disclosure, while remaining transparent to normal, policy compliant activities.

POLICY DEFINED IN BUSINESS TERMS

Policy definition is achieved using intuitive authoring tools that translate business policies into digitized information controls in a fraction of the time and cost of using manual, error-prone techniques. Collaboration between business policy analysts and IT accelerates development and deployment of controls to:

Record: Log details about data handling and disclosure activities for reporting and analysis.

Monitor: Gain insight into healthcare data activity at each point of use to evaluate and quantify risks.

Report: Analyze policy forensic and use activities, patterns and trends by users, policies, and resources.

Notify: Communicate critical events and improper activities to relevant policy stakeholders.

Inform: Educate users with immediate feedback about policies and procedures, and proper disclosure.

Execute: Automate predefined procedures based on important events & actions to assist users in handling healthcare data properly.

Block: Actively prevent improper and harmful activities by enforcing appropriate security policies and HIPAA regulatory governance

POLICY-BASED CONTROLS THAT EVALUATE CONDITIONS

Managing proper data handling is difficult when devices, data, and users are mobile, or if users, customers, and partners are spread across multiple locations. Policies are enforced by evaluating context, such as identity, time and locations, devices used, communication channels, and activities, in real-time, to apply precise protection. Policy sets include:

Healthcare Data Use Discovery

- Monitor how data is accessed and handled, inside and outside the organization, to identify risks.
- Monitor inappropriate disclosure trends to gain insight and investigate potential losses or misuse.
- Monitor data access by unauthorized roles and alert users when access conditions are improper.

Healthcare Policy Education

- Educate users on PCs or laptops to handle data properly, aligned with HIPAA and best practice policies.
- Educate users during export (saving) of healthcare data out of applications to prevent exposure to potential data leakage risks.

Automated Data Handling

- When patient or subscriber data is accessed or disclosed under specific conditions, automatically apply encryption tools to eliminate discretionary use of security.

Healthcare Communications

- Prevent distribution of ePHI during Web or FTP upload, and during communications including email and IM, to ensure it is not received by unauthorized parties.
- When data is distributed outside the organization, such as hospitals to insurers, prevent the saving or copying of data outside of designated (secure) locations.

Maintenance and Auditing

- Audit and report policy compliance to clearly demonstrate HIPAA and best practice goals are met.

RISK ASSESSMENT & REDUCTION

The Solution also allows organizations to gain insight into information access and use activities that create risks, and audit the effectiveness of controls in place. Reports include:

- Daily / Weekly / Monthly - Activity & Policy Compliance Reports
- Access Point Investigations (Use Activities, by Device or System)
- User Workflow Investigations (Use Activities, by User)
- Healthcare Data Risk Assessment (Use Activities, by Data Type)

- Workflow Activity Risk Assessment (Use Activities, by Activity)
- Information Copied and Violations to Removable Media

In addition, the solution allows custom reports to be developed to meet specific policy requirements.

POLICY ENFORCERS

Policy Enforcers that run at various information control points are available from NextLabs and its partners. In addition, custom policy adapters for new or custom applications and systems are easily developed using the Adapter SDK. Typical policy adapters include:

- Windows® desktops
- Windows® file servers
- Microsoft® Office SharePoint® Server
- Microsoft® Outlook®
- Linux desktops or server

INVEST IN A SOLUTION THAT ADAPTS TO YOUR EVOLVING BUSINESS REQUIREMENTS

The Healthcare Data Protection Solution is achieved within existing infrastructure, without changing workflow or user behavior, by using a scalable policy architecture that deploys along with your existing applications and systems. As new devices are added— and as resources, users, applications, and business structure change—policies are automatically updated. Manual changes to the policy model or policy statements are not required. Healthcare organizations gain a complete solution to discover risks, educate users, automate procedures, and protect information from misuse and unauthorized disclosure. Healthcare organizations can now support the safe adoption of new technologies and business initiatives, as the organization continues to evolve.

NEXTLABS® | Zero Trust Data-Centric Security

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit: **http://www.nextlabs.com**.