NEXTLABS

SOLUTION BRIEF

Active Control for ePHI Access and Handling Protection Module

SOLUTION HIGHLIGHTS

- **Addresses common ePHI access and handling risks that result in improper disclosure and policy violations**

  Simplifies and accelerates deployment with predefined policies and reports:

  Targeted, predefined, best-practice policies, ready to deploy

  Quick reports that let you measure policy effectiveness

  Polices and reports that are easy to customize or use as templates

- **Provides pre-designed ePHI access and handling control over:**

  Patient Medical Data

  Subscriber Financial Data

  Patient/Subscriber Benefits Data

  Medical and Financial Records

  Personally Identifiable Information (PII)

Patient and health insurance subscriber electronic protected health information (ePHI) is at risk of violating HIPAA regulations and organizational best practices when it is used in unauthorized ways. To safeguard patient and subscriber data comprehensively requires a top-down, policy-based approach that applies business conditions when ePHI is accessed from servers and used at endpoints to mitigate the risks of improper disclosure.

The Active Control for ePHI Access and Handling Protection Module lets you minimize the risks of ePHI access and misuse with a set of predefined best-practice policies that are easily deployed to apply ePHI controls that meet compliance objectives.

LIBRARY OF BEST-PRACTICE EPHI ACCESS & HANDLING POLICIES

The module provides an extensive set of predefined policies that are closely focused on the specific problems associated with monitoring and protecting ePHI access and handling. The policies cover Access, Storage, Endpoint Device, and Removable Media.

ACCESS POLICIES

Let you control access conditions for a given class of ePHI, automate access procedures to ePHI that are restricted to certain locations, and educate users about where they must (or may not) access certain types of ePHI. Examples include:

- Prevent anyone from accessing patient or subscriber records except from approved network locations and devices that use encrypted connections to data repositories.
- Allow only authorized medical or insurance staff to view specific types of patient or subscriber ePHI based on functional role, during normal operating business hours.
- Educate general staff to only access non-patient data in SharePoint sites and prevent record viewing (regardless of how permissions are defined directly in SharePoint).

- **Provides universal data protection:**

  Cross-platform: Windows and Linux, systems and applications

  User may be connected to the network, or not

  Policies govern even the most privileged users

- **Allows you to monitor and control ePHI:**

  Access and viewing

  Storage

  Encryption

  Sharing

  Printing

  Moving and copying

  Remove/delete permission

  Posting to SharePoint or other document management systems

  Attaching to IM or e-mail

  Cutting and pasting content

  Copying to/from removable drives

  Changing security settings

  Application use

STORAGE POLICIES

Let you control where users may copy, move, and store a given class of ePHI data, automate the handling of data that is restricted to certain locations, and educate users about where they must (or may not) store certain types of data. Examples include:

- Prevent anyone from copying patient or subscriber records to any network location except approved, designated directories where it is automatically encrypted.
- Do not allow anyone to delete subscriber financial data in a specified archive location until a designated date; after that date, allow only authorized users to delete data.
- Only patient ePHI may be posted to a medical records SharePoint site, and only by members of the medical staff (regardless of how permissions are defined in SharePoint).
- Endpoint Device Policies

Let you control how certain classes of ePHI data may be copied to and used on desktop computers, laptop or tablet PCs, and so forth. Examples include:

- Allow users to copy insurance subscriber financial data to approved desktops, but automatically encrypt it before copying.
- Allow ePHI to be copied to authorized medical staff computing devices, but as view-only (no user can move, copy, rename, distribute, print, or copy and paste data).
- Monitor all devices and delete files if a device is determined to be missing or stolen.

REMOVABLE DEVICE POLICIES

Let you control whether and how users may move ePHI to any removable media, such as USB drives, CDs or DVDs, external hard drives, or tape backups. Examples include:

- Allow only medical staff to copy patient records to any removable device, and only within a defined time window; automatically encrypt any files before copying.
- Allow subscriber financial data to be copied to USB drives only from an approved PC and only by authorized claims handling staff.

USING THE MODULE

All Entitlement Management® Policy Application Modules, including ePHI Access & Handling Protection, is deployed in five easy steps.

Step 1: Import Libraries
You start by importing the policy and component libraries into an existing Control Center. Once imported, policies and components are available for use in the Policy Author's design panes.

Step 2: Choose your Policies
Next, browse the policy libraries and select the policies that match the specific endpoint data control challenges you want to solve.

Step 3: Configure your Policies.
Next, configure the policy components required by your selected policies by mapping them to your environment.

Step 4: Deploy to your Network.
At this point, you can deploy the policies out to all relevant Policy Enforcers. All required components are deployed along with the policies, automatically. You can schedule them to take effect immediately or at some future time.

Step 5: Audit Policy Performance.
After importing the library of predefined quick reports, you can use Entitlement Management Reporter to monitor how often, and in what ways, your deployed policies are being enforced. This is helpful for the continuous audit information it provides, and also as a testing tool to confirm that all policies are working as intended.

If you determine that a policy definition needs further fine-tuning, the flexibility of the ACPL policy language and the Policy Author's graphical UI make it quick and simple. In fact, you can easily customize all pre-defined components, policies, and even custom obligations to adapt them to your specialized uses—essentially using them as templates for new tools to serve your information control requirements.

ABOUT POLICY APPLICATION MODULES

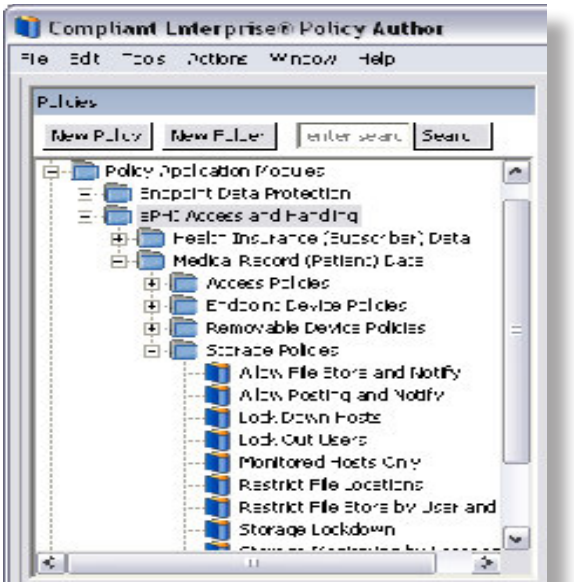
Active Control for ePHI Access & Handling Protection is one of a set of *Policy Application Modules* that run on the Entitlement Management® Active Control System. All modules are simple to install and designed to streamline and accelerate policy deployment by providing libraries of predefined policies designed to solve a specialized information control problem. Each module includes:

- An extensive library of predefined, best-practice policies
- A library of predefined audit reports
- A set of automation obligations that trigger special active responses, such as encrypting, tagging or deleting data, when policies are enforced
- An in-depth implementation and reference guide explaining the design of all predefined elements and how you can use them—whether straight out-of-the-box, or with minimum customization, or as templates for creating your own extended policies and sets

OTHER POLICY APPLICATION MODULES

In addition to Active Control for ePHI Access & Handling Protection, the following modules are now, or will soon be, available:

- Active Control for ePHI Distribution Protection
- Active Control for Information Entitlements
- Active Control for Endpoint Data Protection



Accelerate your ePHI control solutions with a library of extensible, pre-defined policies

- Active Control for IP Protection: High Technology
- Active Control for Business Information Barriers: Financial Services
- Active Control for Business Information Barriers: Aerospace and Defense
- Active Control for IP Protection: High Technology

SYSTEM REQUIREMENTS

- Entitlement Management 2.0 or later
- File Server Enforcer for Windows® or Enforcer for Linux (Recommended), Enforcer for Microsoft Office SharePoint Server or similar Entitlement Management Policy Enforcer for servers
- Desktop Enforcer for Windows (Recommended), Enforcer for Linux, or similar endpoint Policy Enforcer

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based 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, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.

NEXTLABS