

HIPAA

Hitachi ID Solutions Supporting HIPAA Compliance

The Hitachi ID Management Suite

The Hitachi ID Management Suite is an integrated solution for managing user onboarding, security management and deactivation processes. It uses automation, self-service, consolidated and delegated administration to reduce IT support cost, improve user productivity and strengthen security.

Sample Healthcare organizations that use the Hitachi ID Management Suite:

- Blue Shield of California
- Cancer Care Ontario
- Hospital Corporation of America
- Humana Inc.
- Independence Blue Cross
- Indian River Memorial Hospital
- Mount Carmel Health
- Siemens Health Services
- St John's Regional Medical Center
- University of Wisconsin Hospital and Clinics Authority

The HIPAA Challenge

Regulatory compliance with the Health Insurance Portability and Accountability Act (HIPAA) has created significant challenges for healthcare providers and payers. While insurance portability is a uniquely American issue, HIPAA includes requirements for patient privacy protection. Privacy protection is also a requirement in most other, non US jurisdictions. To view the full text of the HIPAA act go to <http://aspe.hhs.gov/admsimp/pl104191.htm>

Privacy protection depends on effective internal controls, including:

- Who can access sensitive patient data?
- How are these users authenticated?
- What can they see and modify?
- Are users held accountable for their actions?

These requirements are met by classic AAA infrastructure: Authentication, Authorization and Audit. AAA infrastructure has been standard in enterprise applications for years. Unfortunately, a large and growing number of applications, combined with high staff mobility have made it much harder to manage user data. As a result, users get access rights inappropriate to their jobs and users may be inadequately authenticated. Problems with user security include:

- Orphan accounts
- Dormant accounts
- Stale or excess privileges
- Weak passwords
- Vulnerable caller authentication at the help desk

These weaknesses are not in the AAA technology -- they are in the business processes for managing user data.

The Solution

Organizations must implement sound processes to manage identities and entitlements, so that only the right users get access to the right data, at the right time. This is accomplished by:

- Correlating different user IDs to people.
- Controlling how users acquire and when they lose security rights.
- Logging current and historic access rights, to support audits.
- Periodic audits of user privileges, carried out by managers and data owners.
- Controlling access to administrative accounts.
- Requiring strong passwords or two-factor authentication.
- Using reliable processes to authenticate callers to the help desk.



Rapid Deployment

Identity management systems can be challenging to implement. Common problems include poor user data quality, costly role engineering and hard to manage workflow systems. To overcome these problems, the Hitachi ID Management Suite:

- Leverages auto-discovery and self-service to find and map login IDs.
- Avoids costly role engineering entirely.
- Simplifies workflow management: one process to authorize all requests.

The Hitachi ID Management Suite

The Hitachi ID Management Suite is an integrated solution for managing user lifecycles. It automates setup, maintenance and termination of user profiles, passwords and access rights. It supports stronger security, and therefore HIPAA compliance, with the following components:

Hitachi ID Automated Discovery

Map user IDs to owners and identify orphan and dormant accounts.

Hitachi ID Password Manager

Enforce a global password policy and ensure that when users forget their password, they are still reliably authenticated.

Hitachi ID Identity Manager

Automatically deactivate access for terminated employees. Report on current and past security rights.

Hitachi ID Access Certifier

Prompt managers, application owners and group owners to periodically review security rights within their scope of authority. Deactivate inappropriate rights.

Hitachi ID Privileged Access Manager

Periodically randomize administrator passwords and control access to those accounts by authenticating, authorizing and logging access.

Technical Specifications

TARGET SYSTEM INTEGRATION

Directory: Windows domains, Active Directory, eDirectory, Novell NDS, any LDAP

File/Print: Windows NT, 2000, 2003; Novell NetWare, Samba, PathWorks, OS2

Databases: Oracle, Sybase, SQL Server, DB2/ UDB, Informix

Unix: Linux, Sun, HP, IBM, Compaq, SGI, Unisys, SCO, DG; passwd, shadow, TCB, Kerberos, NIS, NIS+

Mainframes: MVS/OS390/zOS, VM/ESA, Unisys, Siemens

Minis: OS400, OpenVMS, Tandem

Applications: Oracle, PeopleSoft, SAP; open plug-ins for SQL, ASPs, web services and more

Groupware: MS Exchange, Lotus Notes, Novell GroupWise

Networking: RAS, routers, firewalls

Flexible Agents: Target API, Telnet, TN3270, TN5250, HTTP(S), Web Services, command-line, SQL code, LDAP attributes

SUPPORT INTEGRATION

Automatically create, update and close tickets on:

- Axios Assyst
- SupportSoft SmartIssue
- Magic Service Desk
- Clarify eFrontOffice
- BMC Remedy AR System
- HP Service Manager
- Tivoli Service Desk
- Peregrine Service
- FrontRange HEAT

Additional integrations through e-mail, ODBC, web services and web forms integration.