

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/admnsimp/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.

