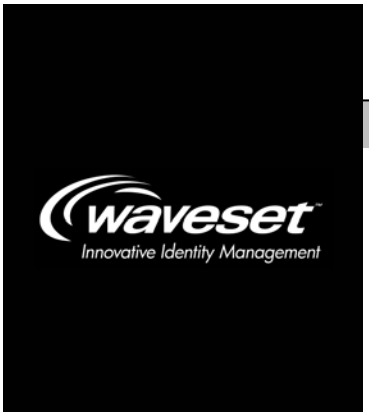

ACHIEVING HIPAA COMPLIANCE WITH IDENTITY MANAGEMENT FROM WAVESET

A white paper written by Doug Landoll, CISSP, CISA of Veridyn

Table of Contents

HIPAA: A TOP EXECUTIVE CONCERN

Healthcare Insurance Portability and Accountability Act (HIPAA) regulations and consumer demand for protection of healthcare information have made the controlling of access to information systems a top concern among IT professionals and corporate executives. Implementing effective and efficient controls to protect the privacy and security of protected health information (PHI) involves coordination and effective use of available technology and products.

In a recent survey of over 800 health care information executives, 56% said they plan to upgrade their systems to become compliant with HIPAA as part of a HIPAA compliance effort. Nearly 100% of all HIPAA compliance teams within organizations include members from the information technology department because of the high reliance on information systems to protect PHI.

It should be no surprise that HIPAA is such a high concern. Nearly every customer, business partner, regulator, and lawyer is looking to the organization's top brass for answers to their HIPAA compliance progress. Looming deadlines, fines of up to $100,000, and prison terms of up to five years for non-compliance elevate the importance of HIPAA compliance as well.

Many organizations are finding that the HIPAA regulations "run deep" and affect many elements of the business process, information system operation, and information system management. In-house solutions of developing policies and procedures from scratch and implementing custom applications and modifications to the existing information systems are time consuming and are typically ineffective. What is needed is a proven solution with HIPAA-compliant features. Using HIPAA-compliant privacy and security features in available technology such as those in Waveset
Lighthouse™ is an efficient and effective way of implementing a HIPAA compliance program within large healthcare organizations.

HIPAA COMPLIANCE IN LARGE ORGANIZATIONS

Due to the number of users, the complexity of data classification, the dynamic nature of organizations, and interconnection of information systems, large organizations have a difficult time supporting HIPAA privacy and security regulations.

- **Many information systems.** The scope of control for PHI is expanded greatly by the sharing of PHI within various information systems within the organization and the sharing of PHI with business associates outside of the organization. Large healthcare organizations share information across a multitude of systems from payroll and patient processing to employee databases and business associate networks. Keeping track of user accounts, patient information, and enforcing appropriate access control policies can be difficult in such far-reaching and heterogeneous environments.
- **Complex roles, data classification and authorization.** To effectively enforce HIPAA Privacy Rules for consent and limiting use of PHI to the minimum necessary, large healthcare organizations must establish and maintain a complex structure of PHI access classes for the data, roles and

privileges for users, and authorization decisions for users' interaction with PHI data.

- **Large and growing number of accounts.** Information systems within large organizations support thousands or tens of thousands of users in a variety of roles. The sheer number of accounts, users, roles and authorization decisions requires effective processes and controls to ensure adequate protection of PHI.
- **Dynamic and volatile nature of accounts.** Frequent changes in who is allowed to access what information multiply the already complex task of access control. Events such as employee turnover, emergency access, promotions, job rotations, and changes in agreements with business associates all require the associated changes in the access control mechanisms. Many of the personnel assigned to these roles change frequently. While other accounts are temporary or require increased level of access for a short amount of time. This dynamic nature of accounts, privileges, and access levels makes the task of account provisioning, maintenance, and termination one of the most difficult tasks in the secure operation of these information systems.

WAVESET LIGHTHOUSE SOLUTION

Waveset Lighthouse facilitates the enforcement of HIPAA privacy and security regulations through the efficient management of identity data, entitlements and permissions. At its core, HIPAA is about taking steps to protect the confidentiality of patient information. Achieving HIPAA compliance means implementing security standards that govern how healthcare plans, providers and clearinghouses transmit, access, and store private health information in electronic form.

HIPAA privacy regulation requires that the use of PHI be limited to that which is minimally necessary to administer treatment. Such limitations must consider the effects various considerations such as provisions for parents and minors, use in marketing, research, payment, and government access on authorization decisions.

HIPAA security regulations further impose requirements to develop and enforce "formal security policies and procedures for granting different levels of access to PH.I" This includes authorization to access PHI, the establishment of account access privileges, and modifications to account privileges. Furthermore, the HIPAA security regulations require the deployment of mechanisms for obtaining consent to use and disclose PHI.

Role-Based Access Controls

Waveset Lighthouse filters access control requests based on Role-Based Access Controls (RBAC) or Rule-Based Access Controls (Rule-BAC). These access control models allow for complex access control decisions to be modeled and implemented in automated systems. RBAC allows for access control decisions to be based on the role currently being performed by an individual.

For example, a physician taking a shift in the emergency room would access the system using his temporary role as an emergency room physician. This would allow the doctor to access emergency room charts and other information required while on duty. When the physician returns to his normal department,

he would access the system using his permanent role as a department chair in the obstetrics ward. This would allow him access to patient information within his department only.

Waveset Lighthouse implements NIST Level 3 RBAC. Level 3 RBAC is defined as an access control system that provides user-role review, role hierarchies, and separation constraints. Level 1 RBAC, or Core RBAC, introduces the basic concept of RBAC where users are assigned to roles, permissions are assigned to roles, and users acquire permissions by being members of roles. Level 2 RBAC, or hierarchical RBAC, adds requirements for supporting role hierarchies. A hierarchy recognizes the concept of senior roles, which acquire the permissions of their juniors, and junior roles, which acquire the user membership of their seniors.

Level 3 RBAC adds the concept of separation of duty. This concept holds that situations of conflict of interest may arise in a role-based system where a user may gain authorization permission associated with conflicting roles (e.g., accounts payable and accounts receivable). Systems implementing Level 3 RBAC enforce a static separation of duty through the enforcement of constraints on the assignment of users to roles.

Effective Account Management

Critical to implementing safeguards to meet HIPAA privacy and security requirements is an effective approach for dynamically managing the many accounts and account privileges required to give access to those who need it and deny access to those who don't. Waveset Lighthouse provides account administrators an effective environment for controlling and enforcing HIPAA privacy and security rules through effective account management. This can be seen by examining the full lifecycle of the account.

- **Account Discovery.** Waveset Lighthouse provides patented mechanisms by which the administrator can understand what accesses already exist on IT systems and applications. An essential element of effective account management is the ability to model the current access rights, analyze them, detect exceptions to corporate policies, and detect and reconcile changes as they occur going forward.
- **Account Management Workflow.** The processes by which accounts are requested, approved, created, modified, and deleted are important elements of account management. The business processes controlling account creation (or "workflow") can be automated and enforced through the Waveset Lighthouse management tools. This workflow enforcement of account creation governs the way in which accounts are requested, the approvals required for account creation, and even enforces certain restrictions on accounts. For example, Waveset Lighthouse workflow controls can restrict an individual from obtaining accounts on the accounts payable and accounts receivable systems thus enforcing the separation of duty principle.
- **Delegated Administration.** Closely associated with workflow, delegated administration is the ability for people outside IT, even end users, to request additions, changes, and deletions to accounts and access permissions. This is facilitated by the workflow and associated business rules so that no HIPAA violations regarding the management of PHI occur. Additionally, this requires a robust and granular authorization model like that found in Waveset Lighthouse.

- **Access Revocation.** Waveset Lighthouse provides the ability to control account privileges through revocation of access rights and monitoring for any changes made outside of the Lighthouse interface. When an individual no longer requires access to PHI, using the Lighthouse interface, the data owner may completely revoke access rights on all accounts associated with that individual. Furthermore, account privilege modifications made outside of the Lighthouse interface are automatically cancelled and accounts are reset to the intention of the data owner within the Lighthouse system.
- **Centralized Resource View.** The way in which data is viewed is critical to the proper management of PHI. For example, Waveset Lighthouse provides the data owner or the auditor both with a ”resource view” of who has access to the information they need to protect, as well as a “user view” that details each user’s privileges.
- Comprehensive Reporting. Waveset Lighthouse provides regular reporting of accounts and account privileges. Typical reports generated by Lighthouse include the presence of dormant accounts on different IT systems and applications, aged or stale passwords, and changes to account attributes and privileges.

Reasonable Safeguards

HIPAA privacy regulations require reasonable administrative, physical, and technical safeguards. Considering the complex and dynamic environment of large organizations, “reasonable safeguards” should include technical tools to ensure PHI access is consistent with established policies and procedures.

- **Automation.** Waveset Lighthouse automates the process of account creation, modification and deletion. In addition to the workflow capabilities previously mentioned, Lighthouse can integrate directly into an HR system or any other authoritative system to get some or all of a user’s information. This integration combined with business logic allows for changes about a user to be propagated with or without human intervention to any or all IT systems or applications.
- **Customized Views.** With Waveset Lighthouse, different administrators, supervisors, and users can have different “views” of the same account information. For example, one person may access a user’s records and see test results without seeing the person’s name. Another person may access a person’s profile information without seeing any medical information. Custom views enable people to see only the data they are authorized to see and block data for which they are unauthorized to see.
- **Policy Enforcement.** Waveset Lighthouse provides a robust Rules Engine which encapsulates the required organizational policies and safeguards so that all account management is performed consistent with those policies.
- **Auditing.** Waveset Lighthouse maintains a complete audit log of all account management activities performed.

Termination Procedures

HIPAA security regulations call for the establishment of effective termination procedures to include changing of locks, removal from access lists and all user accounts, and retrieval of tokens and access cards.

Waveset Lighthouse provides effective tracking of all accesses to PHI for each individual. Such accesses can be user accounts on various systems and under various names, and company issued equipment such as tokens and access

cards. Waveset Lighthouse can quickly and effectively deprovision a user when they leave or change roles within an organization.

Entity Authentication
HIPAA security regulations call for effective entity authentication.
This should include automatic logoff of accounts, unique user identification, strong passwords, and two-factor authentication.

Password Strength Enforcement.
Waveset Lighthouse enforces password strength policies throughout multiple systems. This helps to ensure that the existing identification and authentication mechanisms are used effectively and according to organizational policies.

- Two-factor Authentication Support. Waveset Lighthouse integrates with multiple authentication mechanisms to provide for strong authentication. Rules can be created to force two-factor authentication for accounts with access to specific information.

IMPLEMENTATION OF IDENTITY MANAGEMENT SYSTEMS

It is clear from the previous discussions that identity management systems (IMS) are essential in large organizations to effectively implement a HIPAA-compliant solution. However, the implementation of an IMS in an existing enterprise across multiple systems and even organizations is not without its challenges. Many IMS integration efforts find it difficult to deploy the IMS and to retain existing business processes. With Waveset Lighthouse, these challenges become easier to overcome.

- **Noninvasive Agentless Approach.** Many IMS products require custom agents on each platform for the product to be effective. Large organizations typically find that the various owners of these platforms are hesitant to allow intrusive agents to be added to their production servers. Moreover, these agents can be affected by the newest operating system and application patches necessary to update these servers. When updates occur, new IMS agents must be obtained and reapplied to each of the affected servers. The process of obtaining permission to install agents on production machines and obtaining the latest IMS agents can become time consuming and difficult.
- **Leverage Existing Data Structures.** Many IMS products create additional copies of the existing data structures in order to model and then manage account information. This adds additional PHI, requires additional controls, and unnecessarily complicates HIPAA-compliance efforts.
- **Ease of Use.** Many IMS products can complicate business operations through additional work-arounds, training, and processes to fit the IMS into the organizational processes.
    1) Many IMSs require changes in existing business processes. Organizations that have developed workflows, business processes, and even scripts for implementing many account provisioning procedures will need to redesign their process to adapt to the available processes within the deployed IMS.
    2) Many IMSs may lose integrity of accounts if platform interfaces are ever used. Organizations will need to develop additional procedures to ensure account integrity.

3) Many products require account administrators and managers to learn a new interface with new commands, screens, and reports. Organizations implementing these systems will need to provide training to administrators and managers for new interface, controls, and reports.

The following table represents the safeguards (administrative, physical and technical) required for HIPAA compliance to illustrate the areas in which Waveset Lighthouse can assist in HIPAA compliance.

HIPAA REGULATION ELEMENT	WAVESET FEATURE
Access controls	Implementation of NIST Level 3 RBAC for structured access control.
Audit controls	Comprehensive account review and reporting on current permissions (both from a resource perspective and from a user perspective).
	Complete audit support of the identity entitlement infrastructure allowing administrators to know not only who has access to what currently, but also who had access to what in the past.
Authorization controls	Effective tools for account administrators to enable, modify and disable user permissions to view and edit PHI.
	Dynamic privilege extensions (emergency access) through dynamic pre-defined rules.
	Automation of effective termination procedures.
	Enforcement of approval processes for the granting of modifications to and revocation of access privileges.
	Enforcement of security policies such as authentication controls, permission expiration controls, and password hardness policies.
Data authentication	Workflow process enforces multiple reviews prior to accepting data entry.
Entity authentication	Two-factor authentication support including ID/Password, PKI certificates, ID tokens and biometrics.
Message authentication	Digitally signed email for approval processing and digitally signed transactions/workflows ensure end-to-end authentication.
Alarm/Notification	Notification and automated action on out-of-compliance security policy enforcement such as password expirations, orphan accounts, and separation of duty conflicts.
Audit trail	Digitally signed audit log of all Lighthouse-initiated activities - both manual and automated provide visibility into what activities have been executed by whom.

Waveset Lighthouse is designed to integrate seamlessly with existing businesses processes, controls, and personnel with the following capabilities:

- utilizes a patented discovery process that scans existing systems to build an account index. ActiveSync recognizes any changes and updates the account index
- integrates with existing systems, business processes, and scripts
- provides a comprehensive management system or leverage existing tools
- interfaces created to have the same look and feel as the interfaces that administrators and managers are more familiar with
- implements workflow procedures to ensure appropriate approval processes for account provisioning Waveset Lighthouse utilizes a patented data-less technology to implement IMS controls. Waveset Lighthouse Virtual Identity Manager indexes existing data structures and does not add to or complicate HIPAA assessments. Waveset Lighthouse utilizes a patented agentless technology to implement IMS controls.

WAVESET LIGHTHOUSE: A KEY COMPONENT FOR HIPAA COMPLIANCE

While implementation of a single technology or mechanism cannot completely meet HIPAA privacy and security regulations, the functions and features of Waveset Lighthouse are essential to implementing a HIPAA-compliant operation within organizations, large or small, that exchanges individually-identifiable health information including entities such as:

- Payers
- Providers
- Clearinghouses
- Laboratories
- Billing agencies
- Pharmaceutical and biotechnology companies

Waveset Lighthouse implements many required elements of HIPAA privacy and security regulations. For large organizations, the implementation of these elements requires the use of technology such as Waveset Lighthouse that can efficiently and affectively automate and enforce these elements.

ABOUT WAVESET

Waveset, a leading provider of identity management solutions, enables the real-time enterprise with an integrated suite of management applications that improve enterprise security while maximizing the efficiencies of critical business and IT processes. With a proven ROI track record for Fortune 500 organizations, Waveset delivers real business value through innovative solutions that give you a competitive advantage.

For more information, visit www.waveset.com