Planning and Implementing HIPAA Compliance Activities

ABSTRACT
This article reviews one healthcare network’s HIPAA compliance management approach, detailing findings and trends from the assessment and presenting possible solutions derived from the remediation analysis activities, including fiscal and implementation timing considerations.

Peter Lee and Mary Staley

In September 2001, NorthBay Healthcare System (NBHS) formally initiated assessment activities for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for their two acute care hospitals located in northern California. The readiness assessment resulted in a gap document, detailing compliance deficits in each of the three areas of HIPAA — Transactions, Code Sets, and Identifiers; Security; and Privacy.

Following assessment activities, an analysis of remediation options was completed that included a cost and risk analysis for each potential solution. The solution options were presented to the executive team, who in turn selected the best solutions that would ensure compliance with the regulations while supporting the strategic direction of the organization. Once the selections were approved, a detailed, integrated implementation plan was created that included budget and resource allocation. The assessment through implementation planning activities occurred over a five-month timeframe, with a final plan completed at the end of the year.

Organizational Background
NorthBay Healthcare System is a not-for-profit network of healthcare providers consisting of NorthBay Medical Center and VacaValley Hospital. The hospitals are supported by a centralized data center and operate under a single

KEYWORDS
HIPAA, Education and training, Readiness assessment, Remediation planning, Implementation planning, Implementation budgeting, Project management
set of operational policies and procedures, in addition to sharing management and executive oversight resources.

**Project Approach**

NorthBay initiated its HIPAA compliance management activities by developing a defined plan and conducting a formal proposal process. The plan included five phases, with the end goal to have a complete HIPAA compliance management plan that could then be managed by internal NBHS staff. The foundation of the overall plan was a commitment to awareness, training, and internal resource involvement at each step along the way. The following stages were defined for the purposes of creating a comprehensive HIPAA compliance management plan for the organization:

1. HIPAA Education and Training
2. HIPAA Education for the Core HIPAA Team
3. HIPAA Readiness Assessment
4. HIPAA Remediation Planning
5. HIPAA Implementation Planning and Budgeting

Healthlink, a Houston-based consulting firm, was selected to perform the requested project activities. For the purposes of providing an integrated summary of the actual project activities, the first two steps were included as initial activities of the overall HIPAA Readiness Assessment project.

The following is a review of the activities at the time of article submission, mid-Remediation Planning.

**Readiness Assessment**

**Project Governance.** NorthBay Healthcare System encompasses two acute care hospitals and a foundation that were included in the assessment activities. To support a successful project, NBHS committed to a defined project governance structure. The HIPAA Executive Steering Team (EST) provided executive oversight with operational support from the Project Steering Team (PST). The overall project was managed from the corporate level using the project charter. This governance structure will remain in place for the duration of the project, with expectations to continue the EST as NBHS moves forward with the implementation activities.

**Education and Training.** To fully support the project activities, NBHS believed that the key players would need to be aware of the scope and impact of HIPAA to the organization, as well as the plan, to complete the agreed-upon project activities. Healthlink provided HIPAA education and training for managers across the organization that were involved in the HIPAA assessment and planning process. The objective of this education and training was to help the managers achieve a thorough understanding of the HIPAA regulations, thus enabling them to participate in the overall HIPAA compliance management process.

**Core Team Training.** Beyond the need for an understanding of the HIPAA standards and overall scope of the project, NBHS wanted to ensure that the key players involved in the assessment activities had an even greater understanding of the section of the regulations relating to their specific operational area. Healthlink provided additional HIPAA education and detailed training for the NBHS core HIPAA project team. The objective of the training was to help the team achieve a thorough understanding of the HIPAA regulations so they would have the background needed to directly participate in the data collection activities of the readiness assessment process. Three Core Team Training sessions were held, one for each section of the HIPAA Administrative Simplification standards — Transactions, Security, and Privacy.

**Data Collection.** The project began with the comprehensive collection of data, including: the development of comprehensive inventories for applications; the inventory of host systems; security policies and procedures; and privacy policies, procedures, and supporting documentation, such as consent and authorization forms. The inventories accounted for items that exist at both the enterprise and the local level. This extensive data collection formed the basis for the assessment.

Following the collection of the related inventories, interviews were conducted with key stakeholders to determine the current environment of compliance. For the security side, interviews were conducted with key network and application analysts. Conducting a walk-through of the physical environments at both organizational locations completed the security assessment. For the privacy assessment, team interviews were conducted for the following privacy processes:

- Consent
- Patient Record Access
- Authorization
- Research
- Marketing and Fundraising
- Business Associates

The privacy process interviews brought together stakeholders for each process, from each local facility, to discuss current activities. The interviews were supplemented by a review of current privacy documentation such as policies, procedures, and actual forms, such as consent, authorizations, and Patient Rights and Responsibilities brochures. In addition, a physical privacy assessment was completed by conducting a walk-through of each facility and the related record storage warehouse.

On the application side, NBHS is in the process of replacing the base HIS and opted not to conduct a detailed assessment of the transaction data elements at the onset of the project. To support the concurrent system selection...
activities, Healthlink developed a vendor questionnaire that addressed each section of the HIPAA Administrative Simplification standards for each vendor to complete. The findings from the questionnaire were included in the final decision-making process. Healthlink did assess the applications not being replaced; however, the assessment was minimal due to the small volume of remaining applications with HIPAA implications.

**Analysis.** The following is a review of the high-level findings noted during the Readiness Assessment activities. Readers should consider such findings to be consistent with Healthlink’s findings on similar assessment activities to date.

**Privacy**
- NBHS' level of privacy preparedness was considered “above average,” with significant privacy protections and processes already in place due to past organizational commitment and the presence of strict state privacy requirements.
- Health Information Management is generally closer to being operationally compliant; this is common because their sphere of responsibility has traditionally received more regulatory attention related to confidentiality than most other provider departments.
- All covered entities will need to pay close attention to HIPAA’s detailed administrative requirements, in particular the documentation requirements, which will need to be in place to monitor and control areas such as training, safeguards, disclosure tracking, and release of information. A number of “best practice” areas and documents within NBHS will form the basis for beginning the documentation remediation efforts necessary to meet compliance.
- There were a number of departmental databases identified that contain protected health information with no governing security or privacy policies or procedures.
- NBHS has a decentralized contract management process. Over 150 contracts were identified that may have Business Associate Agreement requirements.

**Security**
- Overall security documentation did not meet all portions of the HIPAA Security standards. This is consistent with other organizations that often have practices in place without documentation to support the potentially compliant practices.
- While network access is tightly controlled, access to applications is less tightly controlled and inconsistent in application. This will be addressed in part in the implementation of the new systems through standard access definitions and parameters.
- Network intrusion detection and auditing is limited, with the need to implement event reporting and response processes.

**Applications**
- The transaction assessment was postponed due to plans to replace the current billing application; however, the replacement system selection activities were delayed, requiring reconsideration of this decision before the end of the project. The decision was made to assess the current billing application for the transaction data elements of current EDI processes, with analysis and recommendations forthcoming.
- Applications containing the required code sets and identifiers will require field length or format adjustments to accommodate the new standards as they evolve.

**Recommendations.** Healthlink provided the following administrative action plan for NBHS and high-level recommendations for privacy, security, and EDI compliance:
- Maintain current governance structure to support ongoing HIPAA compliance management activities into the Remediation Analysis phase.
- Continue to develop a HIPAA compliance program office to coordinate compliance efforts while ensuring HIPAA efforts are in concert with NBHS’ overall strategic plan. Utilize a monitoring system to track progress towards HIPAA compliance. Include HIPAA compliance activities into NBHS Compliance Committee responsibilities.
- Oversee the development of a remediation plan to identify options for compliance. Analyze risks, costs, and benefits of each option to ensure cost-effective and appropriate uses of resources. Develop implementation plans and budget for all remediation efforts. These activities are being conducted as part of the overall NBHS HIPAA Compliance Management project. Emphasis should be on the immediate need to address financial continuance in October 2002, with the ability to conduct current e-business at that time, at a minimum.
- Monitor changes in HIPAA requirements from Congress and the Department of Health and Human Services, in addition to any changes in California state regulations that impact patient privacy.
- Ensure the development and implementation of policies and procedures required by HIPAA using a centralized approach to the development of documentation. NBHS currently has a well-developed policy review process; however, the forms review and approval process has only recently been reinstated. Formal executive support of an expedient forms creation, review, and approval process will assist in the development of HIPAA-compliant documentation such as consents, authorizations, and notice of privacy practice.
- Identify appropriate funding mechanisms to provide necessary capital and operations resource dollars for ongoing HIPAA activities.
- To support the HIPAA Program Office, NBHS should immediately attend to the following recommendations:

1. **Privacy Recommendations**
   - Establish compliant standard language for consents, authorizations, and privacy notices containing all specific language required under the regulations.
FOCUS: HIPAA

NBHS has consents and authorizations from which to begin this activity, but should ensure the removal of all conflicting forms from circulation. Include the development of appropriate mechanisms to implement and track the required documentation to ensure that necessary and/or requested restrictions are honored.

- Formally define the relationship between NorthBay Medical Center and Vaca Valley Hospital for purposes of HIPAA requirements for consent for information use.
- Consider the development of a centralized contract management office to maintain the repository of all contracts that will be impacted by HIPAA.
- Develop and implement the changes required to meet the patient access standards, including the right to access the record, the right to request an amendment to the record, the right to an accounting of disclosures, and the right to restrict information at the centralized HIM departments and the decentralized ancillary departments.
- Develop policies and procedures that address NBHS’ commitment to minimally necessary requirements.

2. Security Recommendations

- Develop security officer role within NBHS.
- Reevaluate disaster recovery plan to ensure each user group has an understanding of the level of service that will be provided during a natural disaster or isolated incident and the timeframes that systems will be restored. In addition, consolidate disaster recovery documentation and conduct routine testing and updating of recovery procedures.
- Establish an organization-wide security training program. Document class attendance and address the curriculum content as required by the regulations using current training documentation procedures maintained in Human Resources. Define approaches for NBHS to meet the “periodic security reminders” HIPAA security requirement.
- Conduct a risk assessment of each instance of generic ID use and the implementation of auto-logoff procedures or password-protected screen savers to ensure workstation security.
- Develop an organizational approach to an integrated security system including access control to parking lots, buildings, restricted areas, computer systems, and so on.

3. Application Recommendations

- Address HIPAA compliance issues with two vendors being considered for the system replacement.
- Perform a return on investment assessment for HIPAA EDI transactions that are not currently used to determine potential savings in implementing these transactions.
- Establish a remediation plan to address deficiencies in Identifiers and Code Sets in all applications to ensure HIPAA compliance.
- Redesign business processes to capture new data elements standardized by HIPAA. Focus on processes involved in admitting, registration, referral certification and authorization, eligibility, billing, payment and remittance advice, and claim status inquiry. Educate staff performing these functions and allow time to assimilate the new processes.

Remediation Analysis

The final report for the Readiness Assessment activities was conducted at the end of October. The purpose of the report was to provide a review of current gaps, provide a high-level action plan, and validate the governance structure recommendations. Based on the findings from the various assessment processes, Healthlink will review all gaps and formulate options for remediation. The options will be based on identified levels of risk and will be presented with a high-level cost benefit analysis. Healthlink will work with NBHS team members to define risks associated with each gap and the proposed solutions, ensuring that solutions fit with the overall strategic direction of the organization.

In defining risk, each gap was assessed based on the following potential impact areas:

- Patient Care
- Financial
- Operations
- Legal and Regulatory

The overall risk was then calculated to determine the overall risk to the organization, and a solution was provided to resolve the risk. Each solution was assessed based on risk and cost to determine the overall most reasonable solution for NBHS as an organization.

The determination of risk was done via a team approach, facilitated by Healthlink, to ensure accurate assessment for the organization. Participants included the same stakeholders who were involved in the assessment activities, with an added feature of combining teams to ensure that technical solutions could be put into operations and operational solutions could be technically supported.

At the time of the article submission, NBHS was in the midst of conducting the remediation analysis activities, so overall results cannot be shared at this time.

Implementation Planning

The expected result of the Remediation Analysis activities is a commitment to a go-forward compliance plan. The Executive Steering Team will be presented with the findings and recommendations of the remediation analysis and will provide executive approval for the development of the overall plan. In the month following the analysis, Healthlink will work with NBHS team members to develop the detailed implementation plan, identifying projects, activities, resources, timeframes, and costs. The plan will be integrated, where possible, with current NBHS initiatives to ensure integration of HIPAA compliance activities in the operations of the organization. The expectation is to have a
FOCUS: HIPAA

plan from which NBHS can manage compliance activities independently of outside assistance, given the ability to support specific projects with internal resources.

In Closing

HIPAA compliance at NBHS will be an integrated process for the facilities governed by the corporate NBHS umbrella. NBHS hopes to take advantage of current processes to support HIPAA compliance, and identify opportunities for improvement through the centralization and standardization of technologies and processes that will support HIPAA compliance as appropriate. The approach taken has been highly successful to date, with visible organizational support from executives, managers, directors, and staff.

The reasons for the high level of success and commitment are believed to be twofold. The first is the foundation of education and awareness for all levels of the organization that was implemented immediately upon project initiation. The second is the detailed project management approach that has been taken, ensuring team involvement and communication throughout the project.

NorthBay Healthcare System believes it is ahead of industry trends in its integrated and coordinated approach to HIPAA compliance. NBHS hopes to use this commitment to ensure that benefits are attained through HIPAA compliance.

About the Authors

Peter Lee is the compliance officer for NorthBay Healthcare System in Fairfield, California.

Mary Staley is vice president of Healthlink in Houston, Texas.

A New Job is Just a Click Away

HIMSS JobMine is an exclusive interactive and integrated online job search for healthcare IT professionals. Whether you are looking for a new job opportunity or searching for a top professional to fill a strategic place on your information and technology team, HIMSS JobMine provides a one-stop search engine to find the perfect match.

Candidates can post resumes, receive e-mailed job alerts, research potential employers, and track their responses to job postings. Reach an audience of top healthcare IT companies and industry facilities with one click of your mouse.

Employers can use resume-searching and posting tools to add, remove, replace, or modify their job postings at any time. Your information will be seen by serious, well-informed candidates who take a proactive approach to career advancement.

Simply log on www.himss.org to access this unique and exclusive online service.