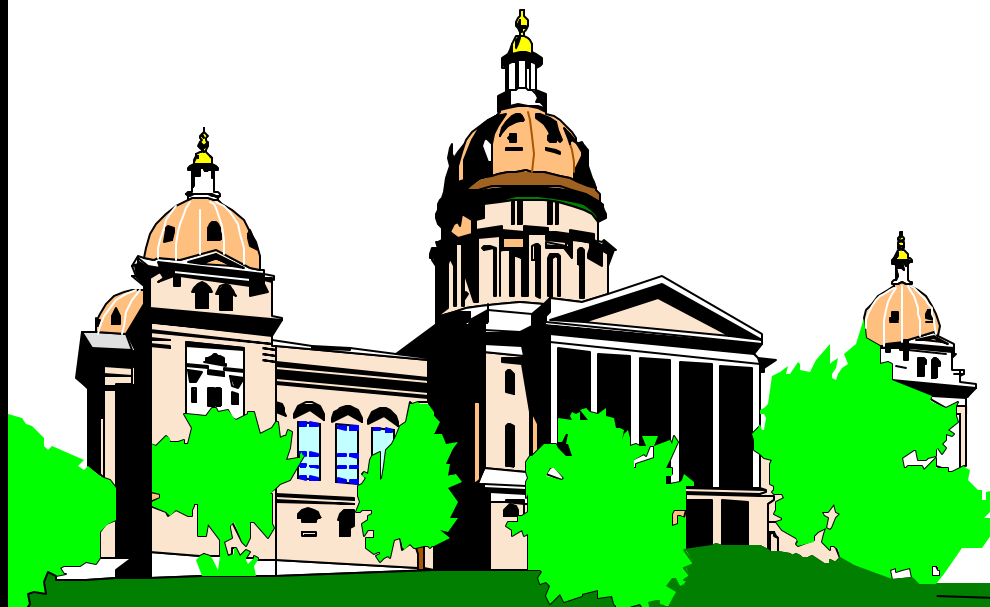


Enterprise HIPAA Compliance

Project Management Charter

November 19, 2001



LOWE

Prepared By: Tom Shepherd
Information Technology Department
401 S.W. 7th St. Suite N
Des Moines, IA 50309-4611
(515) 725-0294
tom.shepherd@itd.state.ia.us



Date: November 19, 2001

Project Name: State of Iowa – Enterprise HIPAA Compliance

State of Iowa – Enterprise HIPAA Compliance Project Management Charter

Table of Contents

| | <u>Page</u> |
|--|-------------|
| Project Scope..... | 3 |
| Business Case..... | 3 |
| Project Objectives | 4 |
| Project Customers..... | 4 |
| Customer Needs | 5 |
| Final Deliverable(s) | 5 |
| Customer Requirements | 6 |
| Life Cycle Stages | 6 |
| Customer Acceptance Criteria..... | 6 |
| Key Stakeholders | 6 |
| Organizational Deliverables | 7 |
| Organizational Acceptance Criteria | 7 |
| Organizational Goals..... | 7 |
| Project Assurance..... | 8 |
| Scope Risk Limit..... | 8 |
| Reviews & Approvals Required | 8 |
| Estimated Project Funding | 9 |

Project Scope

Business Case

The Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 (HIPAA) was passed by Congress to reform the insurance market and simplify health care administrative processes. The administrative simplification part of HIPAA is aimed at reducing administrative costs and burdens in the health care industry by adopting and requiring the use of standardized, electronic transmission of administrative and financial data. HIPAA requires the Department of Health and Human Services (DHHS) to adopt national uniform standards for the electronic transmission of certain health information.

The five specific areas of administrative simplification addressed by HIPAA are:

- Electronic Data Interchange (EDI) - the electronic transfer of information in a standard format between trading partners. It allows partners to exchange information and transact business in a fast and cost-effective way. The transactions that are included within HIPAA consist of standard electronic formats for enrollment, eligibility, payment and remittance advice, claims, health plan premium payments, health claim status, and referral certification and authorization.
- Code Sets - includes data elements used to uniformly document the reasons why patients are seen and what is done to them during their health care encounters (procedures).
- Identifiers - numbers used in the administration of health care to identify health care providers, health plans, employers, and individuals(patients). Over time, this is intended to simplify administrative processes, such as referrals and billing, improve accuracy of data and reduce costs.
- Security - standards need to be developed and adopted for all health plans, clearinghouses, and providers to follow and to be required at all stages of transmission and storage of health care information to ensure integrity and confidentiality of the records at all phases of the process, before, during and after electronic transmission.
- Privacy -standards to define what are appropriate and inappropriate disclosures of individually identifiable health information and how patient rights are to be protected.

Governmental entities will encounter many challenges in their efforts to comply with HIPAA. Government at all levels will be required to make programmatic changes such as altering business processes, adapting to the loss of "local codes" that track the health care needs of specific groups, and modifying practices to ensure patient privacy.

States are currently evaluating impacts of HIPAA through assessments and evaluations. Initial current HIPAA assessments and evaluations by State Medicaid Agencies' are producing the following results:

1. Very few electronic transactions are currently implemented.
2. Existing MMISs will require significant change at both the program and data structure levels.
3. Identifying all of the required changes will be a significant challenge.
4. Significant understanding and assessment of the underlying business policies and rules will be required to correctly integrate HIPAA changes.

One documented data mapping and analysis of existing MMIS files to HIPAA files resulted in only 38% of the required HIPAA fields and elements being accepted by the MMIS. The handling of the additional HIPAA data and resulting data loss with the elimination of local codes will present major redesign, development, and testing issues. Although MMIS systems are different, most of the systems in use today are based on a core set of original models that have been cloned and moved from state to state. Thus, the impacts of HIPAA are comparable for all states.

Failure to comply with HIPAA could result in inefficiencies in the health care delivery system and have a significant fiscal impact on state agencies. Specifically, failure to adopt the national standards could cause service interruptions of major health programs, such as delays or an inability to process provider claims for payment. Additionally, the ability to interact with business partners could also be hindered and leave the agency unprepared for future transaction standards.

Project Objectives

The State of Iowa needs to allocate internal resources for project planning and management, overseeing work activities, assessing policy and procedural needs and maintaining compliance over time in order to become and remain HIPAA compliant within the timelines specified by the applicable rule(s). As of this writing, they are:

1. **Transactions:** The Administrative Simplification provisions of the law require the development and implementation of national standards for electronic health care transactions. Compliance with this rule is set now for October 16, 2002.
2. **Privacy:** The second HIPAA rule deals with Privacy issues. Compliance with the Privacy Rule is required by April 14, 2003. The rule specifies how covered entities and other health organizations transfer, disclose, protect or receive health care information from patients or other parts of the system. In general, these new procedures will preclude any disclosure of personal health information without the active, informed consent of the patient.
3. **Security:** The third rule, which deals with Security issues, has not yet been published in final form. This rule is still not finalized as of November 19, 2001.
4. **National Identifier Codes:** This part of the Act establishes unique identifiers for providers, plans, employers, and individuals. The latter rule (for individual identifiers) has been placed on hold, in part because of concern by privacy advocates over the idea of assigning identity numbers to individuals. The other three rules have not been filed. This would put the compliance date in the 3QFY2004 at the earliest.
5. **Enforcement and Claims Attachments:** These final rules also have yet to be published. Compliance is expected in 2003 or 2004.

For HIPAA covered entities, achieving HIPAA compliance must take priority over other non-HIPAA related initiatives.

Project Customers

HIPAA affects all health plans, health care clearinghouses, and service providers who submit or receive health care transactions electronically. This includes private health insurance plans as well as government medical assistance programs, including programs operated by local government. The project customers are the executive branch agencies in state government.

Assistance will be provided to the legislative and judicial branches for HIPAA-related inquiries and to other governmental entities as resources permit.

Customer Needs

The customers within state government fall into two categories. The first are HIPAA-covered entities that deliver services that meet the HIPAA definition as a health plan, health care clearinghouse, and/or service provider. This group of customers needs to accomplish the following:

- Develop an Assessment Plan and Strategy
- Document Current Systems and Processes
- Perform a Requirements Analysis
- Develop a Risk Assessment
- Develop a Compliance Strategy
- Develop an Implementation Plan

The second group of customers is comprised of the agencies that conduct business with HIPAA-covered entities and are required to comply with policies and procedures established as a result of the HIPAA rules. (Example: State agencies may receive, review, and store an employee's medical records in the in the processing of a Workers Compensation or collect and transmit personally identifiable information used in applying for health insurance coverage.) This group of customers will need education and awareness sessions to ensure they are compliant with existing business associate agreements, policies, and procedures.

The education includes, but is not limited to:

| Topic | Description | Audience |
|--------------------------------------|--|--|
| HIPAA Organizational Processes | Review of policy development and process re-engineering theories and techniques as they relate to HIPAA compliance. | Management and Supervisory Staff responsible for HIPAA process implementation and compliance across State Agencies. |
| Privacy and Security Policy Training | Overview of HIPAA with a strong emphasis on existing and new Privacy and Security policies implemented by the State of Iowa. | Agency privacy and security officers; Clerical staff; Agency Personnel Specialists; Personnel Officers; Professional, Administrative, Technological, Contractor and Temporary Staff providing support to automated personnel administration systems. |

Final Deliverable(s)

- Compliance of all functions within the agency that are covered by the HIPAA definition as a health plan, health care clearinghouse, and/or service provider.
- Designation of a security officer to oversee all HIPAA covered security policies and procedures.
- Designation of a privacy officer to oversee all HIPAA covered privacy policies and procedures.

-
- Implementation of agency-specific change control policies and processes to insure that new information systems and business associate agreements address HIPAA compliance.

Customer Requirements

The deliverables will be acceptable if they create and support environments that are consistent with the standards, requirements, and implementation features outlined in the HIPAA rules.

Life Cycle Stages

- Develop the HIPAA Project Management Office and HIPAA Workgroups
 - Identify a HIPAA representative for each Agency.
 - Determine what in-house resources can be allocated to the project.
 - Identify external resources required for the HIPAA efforts.
- Begin detailed assessments of all state agencies to determine HIPAA coverage status. This assessment will be used to:
 - Develop a scope of work for each agency.
 - Survey business associates to determine their ability to meet the standards.
- Evaluate alternative compliance solutions.
- Conduct HIPAA Awareness and Training Sessions and Rollout HIPAA Implementation Awareness Program to Agency and IT Personnel.
- Develop comprehensive project plan.
- Develop and define a management structure to implement information the appropriate Security Officer and Privacy Officer functions within state government under the auspices of the enterprise security and enterprise privacy offices within the Information Technology Department.
 - Develop a program to monitors compliance with Security/Privacy policies and procedures.
- Implement a change control policy and process to ensure that new information systems, business associate agreements, policies, and procedures address HIPAA compliance.

Customer Acceptance Criteria

Deliverables will be acceptable to the state agency customers if they are in compliance with applicable HIPAA rules within the specified time frame and qualify the customer for all appropriate reimbursements of HIPAA program costs.

Key Stakeholders

Note: As with any public expenditure of funds, the taxpayer is one of the key stakeholders. Their interests are represented by the various groups listed here:

Stakeholders Currently Represented on the Project Team

- Department of Management – Representing the interests of the Governor as well as the financial interests and budget impacts of the project.
- HIPAA-Covered Governmental Entities – Representatives from the agencies that are defined by HIPAA rule as a health plan, health care clearinghouse, and/or service provider.
- Non-HIPAA-Covered Governmental Entities – Representatives from the agencies that do not meet the HIPAA definition as a health plan, health care clearinghouse, and/or

service provider but must meet comply with HIPAA business associate agreements, policies, and procedures.

- HIPAA Legal Counsel
- HIPAA Subject Matter Experts – Specialists and/or technicians specializing in national standards for electronic health care transactions, e-government/e-business, information privacy, information security, medical records, or claims processing.
- HIPAA vendors – This includes contractors, if any, who are directly responsible for HIPAA deliverables.

Stakeholders Not Currently Represented on the Project Team

- Legislature – The legislature will be given regular project updates as well as requests for funding, however, it is not anticipated they will have representation at the project meetings.
- Consumers, Providers, and Insurers of Healthcare Services.

Organizational Deliverables

- Standards-based electronic infrastructure that supports the standardized data format (transactions, code set, and identifier) requirements and realizes cost savings for the payers and providers in government by automating transactions.
- Enterprise security policies for all covered data, processes and procedures.
- Enterprise privacy policies for all covered data, processes and procedures.
- Enterprise change control policy and process to insure that new information systems, business associate agreements, policies, and procedures address HIPAA compliance.
- Business process review and redesign.

Organizational Acceptance Criteria

The organizational deliverables will be acceptable if they result in:

- Automating manual processes (e.g., claims data entry).
- More accurate claim submissions.
- Fewer suspended claims due to missing or misinterpreted information.
- Reduced/eliminated rework.
- Reduced ancillary costs (office supplies, postal costs, and telephone charges).
- Improved business processes that directly impact other healthcare stakeholders.
- Improved quality of service delivery.
- Reduced operational costs.
- Redesigned business processes to improve efficiency and healthcare policy analysis.

Organizational Goals

The goal of the enterprise HIPAA compliance effort is to: a) create an organization whose business operations are compliant with all applicable federal rules; b) realize the efficiencies of electronically processing and exchanging individually identifiable health information (i.e. reduce the number of forms and methods of completing claims and other payment-related documents; implement the use of universal identifiers for providers of health care; and increase the use and efficiency of computer-to-computer methods of exchanging standard health care information); and c) create a working culture that places emphasis on ongoing business process review and redesign and the security and protection of individually identifiable health information.

Project Assurance

Scope Risk Limit

The current assessment for this project is currently High Risk, High Uncertainty. This is due to the following factors:

Financial Uncertainty – Without a completed HIPAA compliance analysis, it is currently not possible to estimate project costs with any reasonable degree of accuracy.

Scope of Work and Time Frames – The scope of work and time frames are dictated by changing federal rules and federal mandates. Most public entities have determined that all systems that require remediation cannot be remediated in the time frame before mandated compliance. As a result, alternate solutions such as translators must be considered. Consequently, many States are remediating systems where necessary and will employ the use of electronic code translators.

Conflicting Priorities - Achieving HIPAA compliance is an imperative and must take priority over other non-HIPAA related initiatives. This will prove difficult in light of the number of mitigating factors (i.e. ongoing welfare reform, downsizing, budget shortfalls, competing for resources with issues such as domestic security and homeland defense).

Reviews & Approvals Required

Once the guidelines are established through the mutual agreement of the stakeholders, the agency plans will be approved and monitored by the Enterprise HIPAA Project Office. Any project plans or expenditures that are outside of acceptable variance criteria must be immediately reported to the Department of Management for assessment and disposition.

Status Reports Required

Agency project status reports for all HIPAA-covered entities must be submitted to the Enterprise HIPAA Project Office on a monthly basis. The project will issue an enterprise project status report on a monthly basis using a color-coded status reporting format.

Estimated Project Funding

The costs associated with HIPAA compliance fall into the following categories:

- HIPAA Compliance Analysis - A compliance analysis for the transactions, code sets, and identifiers; privacy; draft security regulations; an overview of HIPAA compliance issues with existing legacy systems; recommendations to address each identified compliance issue; and a concise Executive Summary identifying key compliance issues that will enable senior management and policy makers to evaluate the IT and business challenges and costs involved in achieving compliance.
- Transactions, Code Sets and Identifiers (TCI) – Electronic data interchange system design and remediation including: enterprise information management solutions; PKI solutions; Virtual Private Networks, conversion to Transaction Formats, conversion to code sets, Identification / modification / implementation of translator programs, validation Testing. The current deadline for transactions and code sets compliance is October 16, 2002. The national identifier rules are not yet final.
- Privacy - Under the auspices of the Chief IT Privacy Officer in the Information Technology Department (Tom Shepherd), implementation of the required privacy regulations and infrastructure including: information privacy policies and procedures to ensure IT assets are afforded the required levels of protection in compliance with the final privacy rules. The current deadline for privacy rule compliance is April 14, 2003.
- Security – Under the auspices of the Chief IT Security Officer in the Information Technology Department (Kip Peters), implementation of the required security regulations and infrastructure including: Internet and intranet penetration analyses; modem dialing/telecommunications connections; functional testing and verification of analysis results; and various security vulnerability analyses; Business Continuity/Disaster Recovery Planning services (including Business Impact Analysis, Recovery Strategy Analysis and Recommendation, Plan Development, Training, Testing/Maintenance), and information security policies and procedures to ensure IT assets are afforded the required levels of protection against destruction, loss, unauthorized access, unauthorized change, or disruption, in compliance with the proposed Security Rules. The HIPAA security rules are not final.
- Training - HIPAA awareness training for management; HIPAA awareness training for operational staff; Security training for employees and HIPAA security officers; Privacy training for employees and HIPAA privacy officers.
- Legal – State preemption analysis, Provider Contracts, Business Partners Contracts. This function is the responsibility of the Office of the Attorney General.

As of November, 2001, the only HIPAA compliance analysis that has been completed within the executive branch of state government was for the Iowa Medicaid Management Information System (MMIS). This included an analysis of the Medicaid program and the following list of users of Medicaid data:

- Federally Assisted Children's Services (FACS)
- Automated Benefit Calculator (ABC) System
- Title XIX
- Individualized Services Information System (ISIS)
- Facilities and Waivers

The estimate for HIPAA compliance for Medicaid in Iowa is \$35 million. The federal Department of Health and Human Services provides funding on the basis of a 90/10 match for HIPAA covered Medicaid expenses. This would require \$3.5 million in state funds and \$31.5 million in federal funding.

The remainder of the Department of Human Services (non-Medicaid) and the other agencies in state government need to complete a HIPAA compliance analysis for an accurate estimate to be compiled. Also, it is the understanding of the enterprise HIPAA project office that the federal Department of Health and Human Services provides funding on the basis of a 50/50 match for non-Medicaid HIPAA covered expenses. Based on comparable program costs in other states and general estimates from various vendor sources, the estimated program costs (in addition to the estimated Medicaid costs above) for the State of Iowa are as follows:

| | |
|---|---------------------|
| Enterprise HIPAA Compliance Analysis | \$ 850,000 |
| Transactions, Code Sets and Identifiers (TCI) | \$10,000,000 |
| Privacy | \$ 6,500,000 |
| Security | \$11,500,000 |
| Training | \$ 800,000 |
| Legal | <u>\$ 1,500,000</u> |
| Total Estimated Non-Medicaid HIPAA Costs | \$31,150,000 |

State funding needed for Non-Medicaid HIPAA (using 50/50 match).... \$15,575,000*

Total estimated Iowa HIPAA costs (Medicaid and Non-Medicaid)..... \$66,150,000

Total state funding needed (Medicaid and non-Medicaid)..... \$19,075,000*

* based on currently projected HHS reimbursement rates.

Please Note:

- This is an estimate of total HIPAA project funding through the 3QFY2004.
- This funding estimate does not provide for aid to local governmental entities or schools.
- The HIPAA project office is working with the Office of the Attorney General to verify federal Department of Health and Human Services reimbursement rates and qualifications for funding.
- As stated earlier, without a completed enterprise HIPAA compliance analysis, it is currently not possible to estimate project costs with any reasonable degree of accuracy.