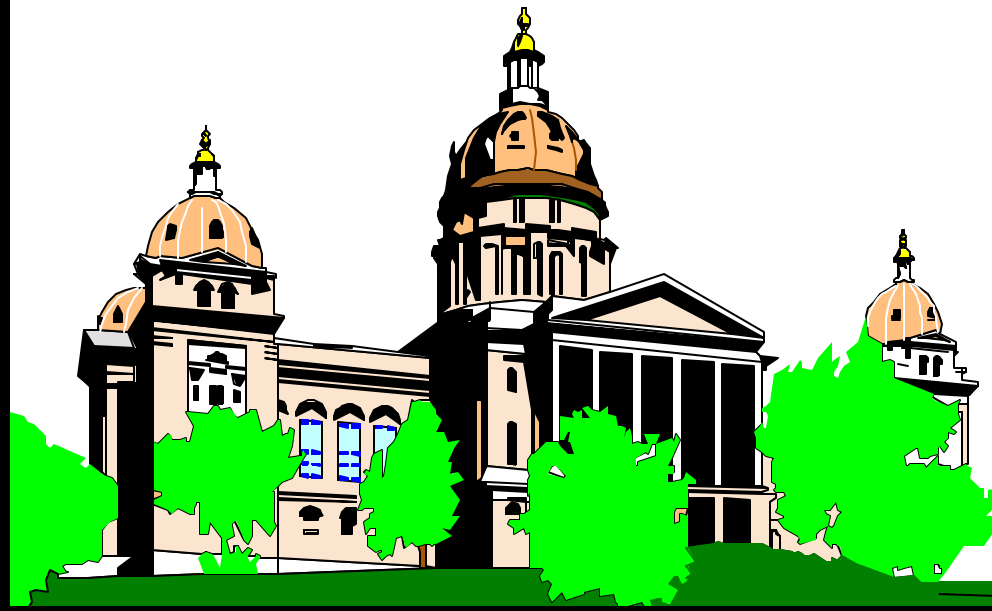


State of Iowa  
Enterprise HIPAA Project Office  
401 S.W. 7<sup>th</sup> St. , Suite N  
Des Moines, IA 50309  
(515) 725-0294

*State of Iowa*

*Enterprise HIPAA Project  
Activities*

*April 5, 2002*



**IOWA**

# State of Iowa HIPAA Project Activities

## Table of Contents

HIPAA Background and Current Deadlines .....	3
HIPAA – Strategic National Implementation Process (SNIP).....	4
HIPAA SNIP Mission.....	4
HIPAA SNIP Purpose .....	5
HIPAA Government Information Value Exchange for States (GIVES).....	6
HIPAA Business Partner RFP .....	7
HIPAA Policies, Procedures, and Technology Research and Development.....	12
Assistant Attorney General's Services.....	13
HIPAA Transactions and Code Sets Deadline Extension.....	13
Enterprise HIPAA Project Office Communication and Information Exchange.....	14
Future HIPAA Activities and Requirements .....	15
Appendix A – Comments on Compliance with the HIPAA Privacy Rule .....	16
Appendix B –Proposed HIPAA Security & Electronic Signature Standards .....	18

## HIPAA Background and Current Deadlines

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996. As part of the Act, Congress called for regulations promoting administrative simplification of healthcare transactions as well as regulations ensuring the privacy and security of patient information. The Act required Congress to enact laws implementing these goals by 1999. When Congress failed to do so, DHHS stepped in and began promulgating regulations. The regulations apply to what are called "covered entities:" healthcare providers, health plans and healthcare clearinghouses who transmit any health information in electronic form in connection with a transaction covered under HIPAA. The regulations are made up of three distinct parts: transaction standards, privacy and security.

**Transaction Standards:** The transactions standards call for use of common electronic claims standards, common code sets and unique identifiers for all healthcare payers and providers. The rules became effective October 16, 2000 and providers originally had two years from that date to comply. DHHS moved the compliance date to October 2003 if a proper compliance plan is filed by October, 2002.

**Privacy Regulations:** The privacy rules govern the release of individually identifiable health information, specifying how health providers must provide notice of privacy policies and procedures to patients, obtain consent and authorization for use of information and tell how information is generally shared and how patients can access, inspect, copy and amend their own medical record. The privacy rules became effective in April 2001 and carry a compliance deadline of April 14, 2003. Key provisions for providers include:

- Consent and authorization requirements
- Opt out provisions
- Minimum necessity requirement
- Administrative responsibilities
- Business associate obligations

Key provisions for individuals include:

- Notice of information practices
- Access to records
- Right to accounting of disclosures
- Right to request amendment to records
- Right to request restriction of uses and disclosures
- Right to request restrictions communicating health information

**Security Regulations:** The security regulations dictate the kind of administrative procedures and physical safeguards covered entities must have in place to ensure the confidentiality and integrity of protected health information. These rules have not been finalized but are expected sometime this year.

## **HIPAA – Strategic National Implementation Process (SNIP)**

A national organization called the Workgroup for Electronic Data Interchange (WEDI) was formed several years ago with the goal of improving healthcare through the implementation of electronic commerce principles and practices. Its mission was to foster widespread support for the adoption of electronic commerce within healthcare. To fulfill that mission, they have worked to achieve the following:

- Provide a forum for the definition of standards, the resolution of implementation issues, the development and delivery of education and training programs and the development of strategies and tactics for the continued expansion of electronic commerce in healthcare;
- Assist healthcare leaders to define, prioritize and reach consensus on the critical technical and business issues which affect the implementation and value of electronic commerce;
- Ensure that electronic commerce standards, policies and regulations for healthcare are thoughtfully developed and implemented;
- Serve as the primary catalyst for the identification, communication and resolution of obstacles that impede the growth of electronic commerce within healthcare; and
- Inform and educate WEDI members and other healthcare stakeholders about the benefits and strategies for successfully implementing electronic commerce.

HIPAA requires specific coordination within the healthcare industry with regard to the privacy and security issues associated with protected healthcare information and the conversion to, and implementation of, a standard set of transaction codes within the healthcare industry. SNIP is a collaborative healthcare industry-wide process resulting in the implementation of standards and furthering the development and implementation of future standards.

### **HIPAA SNIP Mission**

The WEDI HIPAA SNIP Task Group has been established to meet the immediate need to assess industry-wide HIPAA implementation readiness and to bring about the national coordination necessary for successful compliance.

- SNIP is a forum for coordinating the necessary dialog among industry implementers of the HIPAA standards.
- SNIP will identify industry "best practices" for implementation of HIPAA standards.
- SNIP will identify coordination issues leading toward their resolution as industry adopted "best practices."
- SNIP will adopt a process that includes an outreach to current industry initiatives, an information gap analysis, and recommendations on additional initiatives to gap-fill.

## HIPAA SNIP Purpose

- Promote general healthcare industry and government readiness to implement the HIPAA standards.
- Identify education and general awareness opportunities for the healthcare industry and government to utilize.
- Recommend an implementation time frame for each component of HIPAA for each stakeholder [Health Plan, Provider, Clearinghouse, Vendor] and identify the best migration paths for trading partners.
- Establish opportunities for collaboration, compile industry input, and document the industry "best practices."
- Identify resolution or next steps where there are interpretation issues or ambiguities within HIPAA Administrative Simplification standards and rules.
- Serve as a resource for the healthcare industry when resolving issues arising from HIPAA implementation.

Tom Shepherd, the State of Iowa Enterprise HIPAA Project Manager, was one of the founding members of the Iowa Regional SNIP Affiliate (RSA) of WEDI. As a affiliate, the IOWA SNIP:

- Holds meetings monthly that are open to all interested persons seeking to resolve issues through collaboration and consensus.
- Has established an organizational structure and governance protocols. The Iowa SNIP is overseen by a steering committee. Tom Shepherd is co-chair of the Iowa SNIP steering committee. There are 24 steering committee members representing all facets of the healthcare providers and payers as well as representation from state and local government.
- Has created three workgroups. They are devoted to Privacy, Security, and Transactions/Code Sets issues. Each workgroup is divided into sub workgroups and is dedicated to researching and resolving specific HIPAA related issues. There are currently 185 people from across Iowa involved in the sub workgroups. There are 8 representatives from various state agencies on the SNIP workgroups.
- Coordinates issues with the national WEDI SNIP.
- Identifies the goals and objectives of the regional effort and the geographical areas that we represent.
- Is establishing a website to support the Iowa SNIP and is establishing a link to the national WEDI SNIP website.
- Shares with WEDI SNIP, whenever possible, documents and other products created by the regional effort that will be beneficial for other regional efforts to access and use.

The Iowa SNIP brings all parties affected by the HIPAA rules to the table and provides a forum for collaboration and coordination of all HIPAA implementation within the State of Iowa. The Iowa SNIP efforts will dramatically reduce the level of effort and costs of HIPAA implementation for Doctors, Hospitals, Pharmacists, Medical Goods and Services Providers, Insurers, Self-Insured Health Plans. This will translate into lower healthcare costs and a higher quality of service for all Iowans.

## **HIPAA Government Information Value Exchange for States (GIVES)**

The Enterprise HIPAA Project Office is a member of the Government Information Value Exchange for States (GIVES). This is a collaborative state government health care focus group resulting in the sharing of information through a clearinghouse highway and providing a forum for discussing and resolving issues in meeting the Health Insurance Portability and Accountability Act (HIPAA) legislation.

GIVES has been established to meet the immediate need to exchange information, identify common government challenges and share solutions in order to attain HIPAA compliance in the timeframe required. By providing a government-focused network, our goal is to minimize duplicate effort. As part of HIPAA GIVES, Tom Shepherd is participating in groups developing deliverables in the following areas:

- Awareness/Training
- Surveys
- Business Operations - Policies and Procedures
- Impact/Gap Analysis

GIVES is also exploring partnerships among governmental entities in:

- Purchasing HIPAA Privacy and Security educational material
- Collaborative software development and the sharing/reuse of existing HIPAA complaint software.

HIPAA Gives can be accessed on the web at: <http://www.hipaagives.org>

## HIPAA Business Partner RFP

In collaboration with state agencies and the Iowa Attorney General's Office, the Enterprise HIPAA Project Office has developed a HIPAA Business Partner RFP. With HIPAA Project funding for FY03 being uncertain, this RFP is written in such a way that all vendor work performed under the RFP will be based on specifically written statements of work. All contracted services will be defined in statements of work (SOW) that are mutually agreed upon between the contractor and the State. These performance-based statements of work will contain a description of the tasks to be performed by the contractor in terms of required outcomes or results. The contractor will be responsible and accountable for achieving the required results based upon the technical and management approach and internal processes which have been mutually agreed upon between the State and the contractor. The key components of the performance-based SOWs are:

- a. Specific and clearly defined contract goals.
- b. Technical and schedule requirements stated in terms of required results.
- c. Methods of performance measurement.
- d. Clearly established deliverables and reporting requirements.
- e. Mandatory requirements that are based on the State's actual needs.

Those statements of work will only be issued after an assessment of available internal resources has been completed. The RFP states:

The Enterprise HIPAA Project Management Office will provide, to the extent possible, project management and HIPAA technical and legal assistance to all state agencies. The primary responsibility for the following aspects of the Iowa HIPAA compliance project are:

<b>Project Aspect</b>	<b>Primary Responsibility</b>
Project Management	HIPAA Project Management Office
Legal Assistance	Iowa Attorney General's Office
Privacy	Information Technology Department Privacy office
Security	Enterprise Information Technology Security Office
Transaction and Code Sets	State agencies (assisted by contractor)

The party identified above as having primary responsibility will determine the extent to which internal state government resources will be used for the various aspects of the HIPAA Compliance Project. This will depend upon the nature of the work request, skills required, availability of internal resources, and other factors as may be pertinent. They will then identify the external resources required and issue an appropriate statement of work to the HIPAA Services Vendor Partner under this contract. The work to be performed will be under one or more of the activity areas as defined in Section 3.2.A.

This RFP will require the vendor to provide services in from specific service areas. The service areas and examples of deliverables required in each service area are as follows:

- 1) **State and Federal Statutory and Regulatory Requirements and Implementation Consultation:** This activity area shall consist of tasks and deliverables related to IT consultation services for complying with state and/or federal statutory and regulatory requirements and implementation and adherence activities to meet those requirements.

Regulatory requirements and implementation/adherence activities including, but not limited to:

- Enterprise risk/readiness assessment to define the current ability of state government to comply with HIPAA mandates. Compile an inventory of business functions and practices with supporting applications, security systems, and policies and procedures. Identify areas of high risk and gaps in readiness. Describe the current state of readiness, a description of what the compliance should be in state government, and identify the gaps.
- Development of a comprehensive HIPAA Compliance Plan for state government containing, but not limited to, identifying the changes needed to agency business practices, policies and procedures to close the gaps; develop remediation alternatives and recommendations for compliance and an estimate of resources required.
- Review and recommendation of products that can be acquired or purchased that can be used to accomplish HIPAA compliance (e.g., assessment tools, model policies and procedures, etc.).
- Alternatives, recommendations and project plans for individual technical solutions and areas where business process and policy changes are required.
- Identification other Federal and state regulations and requirements that are more stringent than HIPAA and make recommendations on how to resolve the differences. (Note: The Iowa Attorney General's Office, Iowa Bar Association, and other interested groups and associations are currently conducting a HIPAA preemption analysis. This analysis will be available to the contractor to assist with the analysis required in this activity area.)
- Training on ANSI X12N Transaction Standards and standard code sets. Code set training including, but not limited to:
  - Procedure Codes – Physician Current Procedural Terminology (CPT-4), HCFA Common Procedure Coding System (HCPCS), and Current Dental Terminology, 2<sup>nd</sup> Revision (CDT-2)
  - Diagnosis Codes – International Classification of Diseases, 9<sup>th</sup> Revision – Clinical Modification (ICD-9 CM)
  - Drug Codes – National Drug Codes (NDC)
- Assist the State of Iowa's Enterprise HIPAA Project Manager with all aspects of project management including the development of additional RFPs, conducting procurement and

evaluation activities, administration of the project budget, and managing contracted activities. The HIPAA Project Office will be coordinating with the project teams established within the HIPAA covered entities in state government and HIPAA contacts within each of the state agencies.

- A Privacy and Security Gap Analysis. Working with the State of Iowa Information Technology Department's Enterprise Security and Privacy Offices, the contractor shall compile an enterprise-wide risk/readiness assessment of state agency business practices including, but not limited to, policies and procedures for privacy and security requirements and prepare a gap analyses. The HIPAA Project Office will approve the format of the gap analyses report prior to contractor development. The resulting report shall include, but not be limited to, current policies and procedures on privacy and security of health care information within state agencies; identification of the state agency policies and procedures which are not compliant with HIPAA requirements; identification of HIPAA requirements for privacy and security for which state agencies have no current policies and procedures; and recommendations to state agencies necessary for them to comply with HIPAA requirements for privacy and security.
- Review and determine if a governmental entity or program is a HIPAA-covered entity as defined by Title II.
- Determine the requirements and responsibilities of governmental entities under HIPAA for:
  - HIPAA covered entities as employers
  - "Hybrid" entities with a HIPAA covered component – employers that are regulated as "covered entities" because of some secondary function or activity they conduct.
  - Employers as group health plan sponsors.
  - Governmental entities that use protected health information about employees or others (i.e. inmates, patients) obtained from other parties who are themselves covered health care providers or payers governed by HIPAA.

**a) Statutory and Regulatory Requirements and Implementation Consultation Deliverables:**

Agency Transactions and Code Set Gap Analysis Report; HIPAA Assessment Tool(s); Analysis and Impact of Federal and State Health Care Statutes and Regulations Report; HIPAA Compliance Risk Assessment and Risk Reduction Strategies Report; Comprehensive Enterprise HIPAA Compliance Plan; Enterprise Privacy and Security Gap Analysis Report.

Training curricula, training material, and/or presentation material for: ANSI ASC X12N Transaction Standards training; Physician Current Procedural Terminology (CPT4) training; HCFA Common Procedure Coding System (HCPCS) training; Current Dental Terminology – 2<sup>nd</sup> Revision (CDT-2) training; International Diagnosis of Diseases – 9<sup>th</sup> Revision – Clinical Modification (ICD-9 CM) training; National Drug Codes (NDC) training; Training evaluation forms; List of participants, completed evaluation forms, and Certificates of Completion for each participant for each topic at each training session; and Staff Questionnaire.

Individual confidentiality/user agreements for personnel with electronic access to protected health information; technical data access controls; discrete employee-by-employee authorization commensurate with job duties; auditing/monitoring function to detect violations

and impose accountability; discrete identification by name or category of the affected workforce and a tailoring of appropriate training, policies and physical and technical safeguards.

- 2) **Data Exchange Requirements and Implementation Consultation:** This activity area shall consist of tasks and deliverables related to IT consultation services for HIPAA data exchange requirements and implementation of those requirements.

Data exchange requirements and implementation consultation activities including:

- It is important for state agencies to exchange certain health data with each other and private health care providers and payers. HIPAA regulations and other State and Federal statutes and regulations place restrictions on access to, and disclosure of, protected health information. Within the constraints of those restrictions, however, the State of Iowa must determine appropriate means to share information where appropriate. This will require a quality assurance review and analysis of the impact on HIPAA projects and related systems of any standards and/or requirements that have been or may be published by the Information Technology Department (ITD) regarding implementation across state government.
- It will be necessary to develop statewide HIPAA policies and procedures, data sharing agreements, etc. These will require quality assurance review and analysis of data exchange requirements with internal and external electronic systems (e.g. claims clearinghouse, Medicaid Management Information System) and provide consultation and recommendations regarding implementation.

a) **Data Exchange and Implementation Consultation Deliverables:**

Review and analysis of state agency data exchange requirements; policies and procedures for data exchange; data sharing or exchange agreements.

- 3) **Independent Verification and Validation (IV&V) Services:** This activity area shall consist of tasks and deliverables related to Independent Verification and Validation services for HIPAA IT projects.

IV&V services including, but not limited to:

- Evaluation and consultation of HIPAA IT project activities.
- Review, analysis, and recommendations about each project work plan.
- Quality assurance review and analysis of documents and deliverables produced by other independent contractors.
- Participation in project planning and oversight sessions.
- Quality assurance activities and evaluation of implementation of HIPAA IT projects, including a methodology for assessing the costs, benefits, and outcomes for each project.

- Proposal of a resource sharing methodology for state agencies involved in HIPAA project activities as well as resource sharing recommendations by and between executive branch agencies, Board of Regents institutions and facilities and local governmental entities.
- Proposal of resource sharing methodology for production support of multi-agency HIPAA IT projects.
- Completion of status reports of each project that includes, but is not limited to: issues, potential obstacles, and recommendations for project improvements or direction.
- Quality assurance activities and make recommendations on any Request For Proposals (RFP) developed by DOH regarding any IT projects.

**a) Deliverables:**

Attendance and facilitation of HIPAA planning sessions; written reports detailing analysis of agency HIPAA project plans, recommendations, identified problems and/or deficiencies; acceptance of agency project deliverables; monthly status reports; post implementation reviews.

- 4) **Information Technology (IT) Consultation and Facilitation:** The State of Iowa has a Chief Information Officer that is charged with, among other duties, the standardization of information technology systems, policies, and procedures. A CIO Council, consisting of CIO's from each of the state agencies, works with the State CIO to standardize and implement IT activities across state government. The CIO Council meets monthly (the last Thursday of each month). The contractor may be required to perform various research and education functions at the request of the State CIO or CIO Council.

The Information Technology Department has developed a digital government strategic IT Plan (100% E Plan). A detailed work plan is being developed to assure each goal and objective is met. Standardization of IT processes across state government is key to the success of this IT Plan. Planning sessions involving IT staff from across state government will be scheduled periodically. From time to time, the State CIO and/or Department CIOs may require consultation regarding the tasks in the work plan, regarding future planning sessions, and/or consultation and facilitation regarding other IT HIPAA related activities. The State CIO and Department CIOs will request technical and consultation services as needed.

**a) Deliverables:**

Technical Consultation and/or Planning and Facilitation Services, as requested.

The RFP is written to allow governmental entities throughout Iowa (state agencies, other branches of government, and local governmental entities) to buy services from this contract. It also preserves the intellectual property rights for any work product produced under this contract. All work products will be owned by the governmental entity contracting for the work.

## **HIPAA Policies, Procedures, and Technology Research and Development**

The Enterprise HIPAA Project Office has compiled HIPAA summaries and executive briefing materials for legislative and other leaders and has responded to various inquiries from state agencies regarding model policies and procedures. Without complete security rules and no firm deadline, the security requirements will remain a moving target. The Enterprise HIPAA Project Office has been sharing all current information on the various rules, requirements, and deadlines with the various divisions of the Information Technology Department so that they can provide HIPAA compliance consultation to the governmental entities within Iowa.

At the request of the Department of Human Services, Tom Shepherd has met with the Medical Assistance Advisory Council to answer their questions about HIPAA. He also has met with the Department of Human Services HIPAA Project Office and consulted with them on a number of project management and resource issues.

HIPAA requires a level of data integrity and security that has not been present in state information technology systems to-date. HIPAA will require system access controls, user authentication, encryption technology, and extensive physical and data security safeguards. The Information Technology Department has already begun basic in-house research and development on the required technologies (i.e. smart card, public key encryption, biometric devices – fingerprint and iris scanners). We are partnering with various industry leaders in this technology to build the expertise that will be needed to successfully implement these systems.

The Enterprise HIPAA Project Office has provided the Enterprise Information Technology Security Office and the Department of Human Services with model job descriptions for the Security Officer and Privacy Officer positions that are required of every covered entity.

## **Assistant Attorney General's Services**

The Enterprise HIPAA Project Office currently has an assistant attorney General, Janet Hoffman, under contract for about 60% of her time. The \$55,000 for this FY02 contract is being paid using Pooled Technology Funds. Janet has dedicated much of her time to developing expertise in the HIPAA legal issues (a rare commodity). Janet provides legal advice and assistance to the Enterprise HIPAA Project Office as well as HIPAA specific advise and counsel to state agencies with HIPAA concerns.

Janet Hoffman is a member of the Iowa HIPAA SNIP Steering Committee and also serves on the Privacy Committee. She is a member of a team of Iowa attorneys being coordinated through the Iowa Bar Association that is conducting a preemption analysis. This analysis will identify which state laws and administrative rules have been preempted by the federal HIPAA law and the Department of Health and Human Service's HIPAA rules. This preemption analysis is absolutely critical to an effective agency by agency HIPAA assessment and gap analysis. The preemption analysis is also essential to the reasonable and proper implementation of the HIPAA rules in the private sector (hospitals, doctors, pharmacists, medical goods and services providers, and medical claims payers). It is anticipated the completed preemption analysis will be available in May, 2002.

It should be mentioned that in most states, this preemption analysis is being conducted by private law firms and legal services companies. The analysis is then sold to each party needing access to the information (tens of thousands of customers in large states) for prices ranging from \$75,000 to over \$400,000 per copy. In Iowa this preemption analysis is a cooperative effort among government and private lawyers and is a volunteer effort. The result of this preemption analysis will be freely available to all who need it in Iowa. This will keep HIPAA implementation costs lower in Iowa and benefit every one in the state. Janet Hoffman is able to spend the necessary time on this preemption analysis by having part of her salary funded by the service contract with the Enterprise HIPAA Project Office.

## **HIPAA Transactions and Code Sets Deadline Extension**

The Enterprise HIPAA Project Office worked extensively in October, November, and December, 2001 with Phil Buchann and Jeff Hood at the Iowa Federal and State Relations Office in Washington D.C. in providing information to members of Congress related to the legislation to extending the deadline for the implementation of transactions and code sets.

The project office also worked directly with Senator Grassley and Senator Harkin's office and the National Governor's Association to provide information related to this legislation.

## **Enterprise HIPAA Project Office Communication and Information Exchange**

The Enterprise HIPAA Project Office currently has an IOWA State Government HIPAA website under construction. Agencies have inquired about the availability of a website. They find that a website is a very effective tool for communicating project plans, project documents, draft policies and procedures, and other pertinent information related to their HIPAA activities. This website should be available the week of April 22, 2002 and will be funded from the Pooled Technology project office funds.

The Enterprise HIPAA Project Office has also completed a number of surveys for various organizations that report the status of our efforts in Iowa. The project office functions as a point of contact for such HIPAA inquiries, vendor contacts, and coordination with other states on HIPAA activities.

The Enterprise HIPAA Project Office has also consulted with various healthcare providers around the state concerning HIPAA covered business practices. One such example was a call from Mr. Aaron Sloan from the Northwest Iowa Drug Treatment Unit. The Juvenile Court was routinely sending him treatment orders and patient information (including criminal case numbers and social security numbers) using unsecured e-mail. Once Mr. Sloan's concerns were understood, the issue was resolved by contacting Larry Murphy at ICIS and agreeing upon a more secure means of transmitting the information. Mr. Sloan will also participate in the Iowa HIPAA SNIP Privacy Workgroup.

## **Future HIPAA Activities and Requirements**

The deadlines for HIPAA are fast approaching. We are required to comply with the Privacy Rules by April, 2003 and the Transactions and Code Sets by October, 2003 (assuming that the covered entities have files a request for extension).

### **Future Activities (Near Term – 1 to 6 months)**

- Issue the HIPAA Vendor Partner RFP (Mid-April)
- Process HIPAA deadline extension request for all HIPAA covered entities in State Government
- Finalize State Law Preemption Analysis
- Conduct State Agency HIPAA Assessments
- HIPAA Compliance Risk Assessment and Risk Reduction Strategies Report
- Enterprise Privacy and Security Gap Analysis Report
- Comprehensive Enterprise HIPAA Compliance Plan
- Enterprise Privacy and Security Gap Analysis Report
- Develop Internal Audit Standards for HIPAA Compliance

### **Future Activities (Long Term – 7 months to 3 years)**

- Ongoing HIPAA Project Progress Reporting
- Completion of HIPAA Project Activities
- Audit of HIPAA Privacy Policies and Procedures
- Testing of HIPAA complaint Transactions and Code Sets
- Training of targeted employees in HIPAA compliance procedures

The HIPAA project work (Medicaid and non-Medicaid) will require funding across the executive branch of state government. Once the assessment is complete, the level of effort required and amount of money needed can be accurately estimated.

## **Appendix A – Comments on Compliance with the HIPAA Privacy Rule**

The largest cost items are the requirement to have a privacy official and the requirement that disclosures of protected health information only involve the minimum amount necessary. It is estimated that over the period 2003 to 2012, 13.6 percent, or \$2.4 billion, of the privacy regulation's total cost will accrue to state and local governments. Of the \$2.4 billion state and local government cost, 19 percent will be incurred in the preparation for the regulation's first year (2003). These costs reflect the change that affected organizations will have to undertake to implement and maintain compliance with the requirements of the rule and achieve enhanced privacy of protected health information.

The costs associated with implementing the requirements under the HIPAA Privacy Rule will be directly related to the number of affected entities and the number of affected transactions in each entity. There are approximately 12,200 health plans (including self-insured employer and government health plans that are at least partially self-administered), 6480 hospitals, and 630,000 non-hospital providers that will bear implementation costs under the final rule.

The largest initial costs resulting from the final Privacy Rule stem primarily from the requirement that covered entities use and disclose only the minimum necessary protected health information, that covered entities develop policies and codify their privacy procedures, and that covered entities designate a privacy official and train all personnel with access to individually identifiable health information. The largest ongoing costs will result from the minimum necessary provisions pertaining to internal uses of individually identifiable health information, and the cost of a privacy official. In addition, covered entities will have recurring costs for training, disclosure tracking and notice requirements. A smaller number of large entities may have significant costs for de-identification of protected health information and additional requirements for research.

### **HHS Comment on Costs to State and Local Governments**

In addition to HIPAA covered entities, the HIPAA Privacy rules will have a cost effect on various state and local agencies that administer programs requiring the use of individually identifiable health information. Non-covered agencies or programs that handle individually identifiable health information, either under permissible exceptions to the disclosure rules or through an individual's expressed authorization, will incur costs in complying with provisions of this rule. Samples of state and local agencies or programs encompassed by the broad scope of this rule include: Medicaid, state Hospitals and Clinics, county hospitals, state mental health facilities, state or local nursing facilities, local health clinics, and public health surveillance activities, among others.

The greatest cost and administrative burden on the state and local government will fall to agencies and programs that act as covered entities, by virtue of being either a health plan or provider, such as Medicaid, state Hospitals and Clinics, and county hospitals. These and other health insurance or provider programs operated by state and local

government are subject to requirements placed on covered entities under this rule. Many of these state and local programs already afford privacy protections for individually identifiable health information through the Privacy Act. For example, state governments often become subject to Privacy Act requirements when they contract with the federal government. This rule is expected to create additional requirements beyond those covered by the Privacy Act. Furthermore, we anticipate that most state and local health programs will, to some extent, need to modify their existing Privacy Act practices to fully comply with this rule. The cost to state and local programs that function as health plans will be different than the private sector, much as the federal costs vary from private health plans.

A preliminary analysis suggests that state and local government costs nationally will be on the order of \$460 million in 2003 and \$2.4 billion over ten years. We assume that the proportion of the privacy regulation's total cost accruing to state and local governments in a given year will be equivalent to the proportion of projected state and local costs as a percentage of national health expenditures for that year. To estimate these proportions, we used the Health Care Financing Administration's November 1998 National Health Expenditure projections of state and local health expenditures as a percent of national health expenditures from 2003 through 2008, trended forward to 2012. Based on this approach, we assume that over the entire 2003 to 2012 period, 13.6 percent, or \$2.4 billion, of the privacy regulation's total cost will accrue to state and local governments. Of the \$2.4 billion state and local government cost, 19 percent will be incurred in the regulation's first year (2003). In each of the out-years (2004-2012), the average percent of the total cost incurred will be about nine percent per year. These state and local government costs are included in the total cost estimates discussed in the regulatory impact analysis.

## Appendix B –Proposed HIPAA Security & Electronic Signature Standards

### Security and Electronic Signature Standards (Summary)

#### Requirements

#### Components

#### **I. Administrative Procedures:**

1. Certification of compliance
2. Chain of trust partner agreement(s)
3. Business Continuity Plans
  - Applications and data criticality analysis.
  - Data backup plan.
  - Disaster recovery plan.
  - Emergency mode operation plan.
  - Testing and revision.
4. Formal mechanism(s) for processing records in compliance with HIPAA
5. Information access control
  - Access authorization.
  - Access authentication.
  - Access modification.
6. Internal audit(s)
7. Personnel security
  - Assure supervision of maintenance personnel by authorized, knowledgeable person.
  - Maintenance of record of access authorizations.
  - Operating, and in some cases, maintenance personnel have proper access authorization.
  - Personnel clearance procedure.
  - Personnel security policy/procedure.
  - System users, including maintenance personnel, trained in security.

## Security and Electronic Signature Standards (Summary)

### **Requirements**

### **Components**

- |                                       |   |
|---------------------------------------|---|
| 8. Security configuration management. | <ul style="list-style-type: none"><li>○ Documentation.</li><li>○ Hardware/software installation &amp; maintenance review and testing for security features.</li><li>○ Software/hardware Inventory.</li><li>○ Security testing.</li><li>○ Virus checking.</li></ul>  |
| 9. Security incident procedures       | <ul style="list-style-type: none"><li>○ Report procedures.</li><li>○ Response procedures.</li></ul>   |
| 10. Security management process       | <ul style="list-style-type: none"><li>○ Risk analysis.</li><li>○ Risk management.</li><li>○ Sanction policy.</li><li>○ Security policy.</li></ul>   |
| 11. Termination procedures            | <ul style="list-style-type: none"><li>○ Combination locks changed.</li><li>○ Removal from access lists.</li><li>○ Removal of user account (s).</li><li>○ Turn in keys, token or cards that allow access.</li></ul>  |
| 12. Training                          | <ul style="list-style-type: none"><li>○ Awareness training for all personnel (including mgmt).</li><li>○ Periodic security reminders.</li><li>○ User education concerning virus protection.</li><li>○ User education in importance of monitoring log in. success/failure, and how to report discrepancies.</li><li>○ User education in password management.</li></ul> |

## **II. Physical Safeguards**

- |                                     |   |
|-------------------------------------|---|
| 1. Assigned security responsibility |   |
| 2. Media controls                   | <ul style="list-style-type: none"><li>○ Access control.</li><li>○ Accountability (tracking mechanism).</li><li>○ Data backup.</li><li>○ Data storage.</li><li>○ Disposal.</li></ul> |

Security and Electronic Signature Standards (Summary)

**Requirements**

**Components**

3. Physical access controls (limited access)

- Disaster recovery.
- Emergency mode operation.
- Equipment control (into and out of site).
- Facility security plan.
- Procedures for verifying access authorizations prior to physical access.
- Maintenance records.
- Need-to-know procedures for personnel access.
- Sign-in for visitors and escort, if appropriate.
- Testing and revision.

4. HIPAA policy/guidelines on work station use

5. Secure work station location

6. Security awareness training

**III. Technical Security Services:**

1. Appropriate Access control (*Including a procedure for emergency access*)

Context-based access

**OR**

Role-based access

**OR**

User-based access

Encryption (as required).

2. Audit controls

3. Authorization Control

Role-based access

**OR**

User-based access

4. Data Authentication

Security and Electronic Signature Standards (Summary)

**Requirements**

**Components**

5. Entity Authentication

Automatic logoff  
OR  
Unique user identification  
  
AND  
  
Biometric OR  
Password OR  
PIN OR  
Telephone callback OR  
Software Token

**IV. Technical Security Mechanisms:**

1. Communications/network controls

**Requirements for all networks:**

- Integrity controls AND
- Message authentication AND
- Access controls

OR

- Encryption

**Requirements for networks with external access:**

- Alarm.
- Audit trail.
- Entity authentication.
- Event reporting.

**V. Digital Signature Requirements**

## Security and Electronic Signature Standards (Summary)

### **Requirements**

1. Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional.)

### **Components**

- Continuity of signature capability (electronic signature is maintained with electronic document.)
- Ability to accept electronic countersignatures.
- Independent verifiability of electronic signature.
- Interoperability.
- Message integrity.
- Ability to accept multiple electronic signatures on a document.
- Non-repudiation.
- Transportability.
- User authentication

For the entire text of the proposed Security and Electronic Signature Standards, visit:  
<http://aspe.os.dhhs.gov/admsimp/nprm/seclist.htm>