Federal Health Insurance Portability and Accountability Act Compliance – Phase 2

FY2004 Request: **$1,656,300**
Reference No: **35721**

AP/AL: Appropriation
Project Type: Transitional
Category: Health/Human Services
Location: Statewide
Contact: Larry Streuber
House District: Statewide (HD 1-40)
Contact Phone: (907)465-1870
Estimated Project Dates: 07/01/2003 - 06/30/2008

Brief Summary and Statement of Need:
The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the Federal government in 1996. Deadlines for compliance with regulations concerning electronic transmission, privacy and security of patient and health care information will be set over the next five years. Substantial monetary and civil penalties can be imposed as a result of non-compliance. The Department is compelled to implement in-depth impact analysis and requirements assessments for its health care programs, operations, computer systems and policies and procedures. It is anticipated that both small and large-scale modifications to systems, operations, policies and procedures will be required.

Funding:	FY2004	FY2005	FY2006	FY2007	FY2008	FY2009	Total
Fed Rcpts	$828,150	$151,050					$979,200
G/F Match	$828,150	$151,050					$979,200
Total:	$1,656,300	$302,100	$0	$0	$0	$0	$1,958,400

☑ State Match Required ☐ One-Time Project ☐ Phased - new ☑ Phased - underway ☐ On-Going
50% = Minimum State Match % Required ☐ Amendment ☐ Mental Health Bill

Operating & Maintenance Costs:

	Amount	Staff
Project Development:	0	0
Ongoing Operating:	0	0
One-Time Startup:	0	
Totals:	0	0

Additional Information / Prior Funding History:
CH1/SSSLA02/P40/L22 $438.8 GF & $438.8 Federal

Project Description/Justification:
The scope and needs of the Health Insurance Portability and Accountability Act (HIPAA) project have changed to some degree from FY2003 due to reduced funding. The issues of timing and funding for transactional solutions have become more critical with the completion of the department's high-level HIPAA assessment and transaction and privacy gap analysis in July, 2002. These issues will likely impact the distribution of funds in the FY2003 and FY2004 project budget.

Nine significant DHSS program areas have been recently identified to have medical claims processing requirements that do not fall within the scope of the new Medicaid Management Information System (MMIS) reprocurement and implementation project. Because the new MMIS will not provide a HIPAA compliant solution, these programs now have an obligation to develop (or purchase), test and implement electronic medical transactions processing system(s) prior to October 16, 2003 to comply with federal regulation and avoid the substantial monetary penalties for non-compliance. Business operations for these program areas will also be impacted if compliant systems are not in place by the specified deadlines, as it is anticipated that most, if not all, of the large providers that these programs interact with will be ready to conduct compliant electronic transactions by the deadline.

FY2004 funding is necessary to complete the transactional requirements and to implement and complete the required tasks to ensure that the department is ready to meet the HIPAA security regulation and standardized identifier deadlines.

HIPAA Compliance Project Phase 2

Summary:

The Federal government enacted HIPAA in 1996. Deadlines for compliance with regulations concerning the electronic transmission and the privacy and security of patient and health care information will be set over the next two to five years. Substantial monetary and civil penalties can be imposed as a result of non-compliance or wrongful disclosure of information after deadline dates.

In FY2003, the Department of Health and Social Services began implementation of in-depth transactional and privacy impact analysis and requirements assessments for its health care programs, operations, computer systems, and policies and procedures. The assessment efforts for privacy and transactions are nearly complete and analysis of privacy impact is complete. The development of requisite privacy policy and procedure, modification of contracts, and procurement and implementation of staff training are well on the way.

The Department must still purchase or develop and implement HIPAA compliant systems for a number of program areas which process health care claims. We also anticipate the need for data conversion to compliant systems. Additionally, the Department will transition from privacy assessments to the necessary assessment and analysis needed to determine impact of the HIPAA security regulations.

This project will procure the services of one or more consulting firms to assist with in-depth security impact and needs assessments. This project may purchase or fund the development and implementation of one or more HIPAA compliant claims management systems.

Detail:

HIPAA was enacted in 1996 as part of a broad Congressional attempt at incremental healthcare reform.

Some portions of the law took effect immediately, providing access to health care coverage and guaranteeing patient rights under employer plans. Other regulations, pertaining to administrative simplification, privacy and security of patient and health information are just now being finalized and will be enforced over the 2003-2005 time frame.

The regulations will impact all health plans, health care providers, health care payers, health care business associates, health care clearinghouses, government medical assistance programs and other organizations involved with directly providing health care, the provision of health care, health care financial transactions, or the handling of health care information. The proposed regulations protect health information that 1) identifies an individual, and 2) is maintained or exchanged electronically, in paper, or oral format. The regulations also provide basic rights for individuals with respect to their protected health information.

HIPAA has been compared with Y2K, in that it is seen as an enterprise-wide issue. However, unlike Y2K, HIPAA is not an information technology issue alone. There are legal, regulatory, process, security and technology aspects to each proposed rule that must be carefully evaluated before implementation plans can begin. Additionally, the HIPAA mandates will continue to impose major changes to current business practices and data handling procedures, requiring extensive retraining of personnel and retooling of business environments.

The new HIPAA regulations that DHSS and other impacted State agencies will be required to focus on are these:

1. Electronic Transactions and Code Sets: The new transaction regulations are an effort to reduce paperwork and increase efficiency and accuracy through the use of standardized financial and administrative transactions and data sets. Some common affected transactions include claims, eligibility and enrollment verification, diagnoses and patient services, procedures, and physician services.

   It became obvious in early 2002 that, on a national level, health plans and providers were administratively and financially unprepared to meet the October 2002 deadline. Therefore, the compliance date for this regulation has been extended to October 2003.

2. Privacy: This regulation specifies how health care entities and business partners of health care entities transfer, receive, handle, protect and disclose protected health information (PHI). The regulation applies to all forms of PHI, whether paper or electronic.

   Health care entities are required to create privacy-conscious business practices and data systems, including the requirement that the minimum amount of health information necessary to conduct business is used or disclosed. Health care entities must:

   1. Ensure the internal protection of individual health information and implement physical and administrative safeguards.
   2. Implement procedures that limit the use and disclosure of PHI to meet the "minimum necessary" standards.
   3. Develop mechanisms for the accounting and auditing of all disclosures made for purposes other than treatment, payment or operations.
   4. Establish policies and procedures to allow individuals to inspect, copy or correct their health information.
   5. Establish contracts and agreements with business associates that ensure the protection of PHI that is shared or traded.
   6. Provide privacy training to members of its work force who have access to PHI.
   7. Establish policies and procedures to allow individuals to log complaints about the entity's information practices.
   8. Designate a privacy official.
   9. Create and make available documentation regarding compliance with all requirements of the regulation.

   The compliance date for the Privacy Regulation is April 2003. The Department is actively engaged in the processes required to ensure that the Department is compliant in all privacy requirements by the April 2003 deadline.

3. Security: This rule applies to the administrative procedures, technical and physical safeguards to ensure the integrity, confidentiality and availability of protected health information. The proposed security standard is divided into four categories:

   - Administrative procedures: These are documented, formal procedures for selecting and executing information security measures. The procedures also address staff responsibilities for protecting data.
   - Physical Safeguards: These safeguards protect physical computer systems and related buildings and equipment from fire and other environmental hazards as well as intrusion. It addresses the use of devices and administrative measures to control access to computer systems and facilities.
   - Technical data security services: These include the processes used to protect, control and monitor information access.
   - Technical security mechanisms: These include processes used to prevent unauthorized access to data transmitted over a communications network.

   As with the Privacy Rule, the Security Rule will require assessments, analysis and documentation regarding compliance with all the requirements. The Security Rules have not been yet finalized, but compliance is anticipated to be late 2004 or early 2005.

4. Unique Identifiers: This rule will mandate the use of unique standard identifiers for providers, health plans, employers and, perhaps, individuals as well. Only the employer identifier has been finalized. Compliance for the others is expected sometime between 2003-2005.

Even though some HIPAA standards are still being finalized, DHSS and impacted State agencies must move quickly to develop and implement compliance plans.

It is expected that funding will be utilized for contractual services for assessment, planning and implementation of programmatic and operational improvements and modifications required by the new laws.

2004	**EDI Standards (Transactional Requirements) & Security Standards**	
	Administration and Management	196,300
	Transactional Requirements	
	Hardware	
	Purchase Servers, Drives, Backup Devices for claims processing	150,000
	Software	
	Purchase software system to handle claims processing needs	300,000
	Security Standards	
	Contractual	
	Legal Support for Review of Current and New Security Policies and Policy Development	80,000
	Security/Vulnerability/Intrusion Testing & accreditation	30,000
	Security Awareness Training and Education	150,000
	Software	
	Software development tools	90,000
	Software modifications to current data systems to support Auditing and Audit Management	200,000
	Purchase of encryption software	230,000
	Purchase and/or Upgrade of Intrusion and Access Control Detection, Prevention & Management Software	90,000
	Hardware	
	Physical Site Security Additions/Improvements	100,000
	Purchase of Additional Disk Resources (or upgrade) for Audit/File Storage and Maintenance Requirements	40,000
	FY 2004 Totals	**1,656,300**
2005	**National Identifiers**	
	Administration and Management	152,084
	Contractual	
	Software modifications to current data systems to support National Identifier database modifications	150,000
	FY 2005 Totals	**302,084**

The new transactional requirements require specific Department programs to be able to accept health care transactions (such as claims, eligibility inquiries, enrollment verification and pre-authorizations), electronically. Most providers will be in position to provide this data electronically by the mandated dates, and Department programs will have to be able to accept the data electronically. Electronic transactions improve the efficiency, accountability, accuracy and administrative and maintenance costs of claims processing for providers allowing them to improve services and reduce costs.

Programs impacted by transactional requirements:
Maternal Child Family Health - Genetics
Maternal Child Family Health - Health Care Program (Children with Special Needs)
Maternal Child Family Health - Specialty Clinics
Maternal Child Family Health - Breast and Cervical Health Check
Maternal Child Family Health - Newborn Metabolic Screening
Maternal Child Family Health - Family Planning
Division of Mental Health and Developmental Disabilities - Alaska Youth Initiative

The implementation of security measures will provide a higher level of reassurance and accountability to the public regarding the confidentiality and ability to secure sensitive health information.

Preliminary assessments may reveal the need for increased funding to handle additional hardware, software, or contractual needs to assist DHSS and other involved State agencies in meeting ongoing HIPAA compliance requirements.

Substantial monetary and civil penalties can be imposed by the Federal Government as a result of non-compliance or wrongful disclosure of information after deadline dates. Program areas, which rely on Federal funding, may also be adversely impacted as a result of non-compliance. In addition, programs will not be able to pay claims in a timely manner to providers.