REPORT TO THE TWENTY-THIRD HAWAII STATE LEGISLATURE 2005

IN ACCORDANCE WITH THE PROVISIONS OF ACT 41, PART III, SECTION 36.1, SLH 2004 ON THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

DEPARTMENT OF HUMAN SERVICES
NOVEMBER 2004

REPORT ON ACT 41, PART III, SECTION 36.1, SLH 2004 ON THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

This document is a report to the Twenty-Third Legislature, 2005, State of Hawaii, made pursuant to Act 41, Part III, Section 36.1, Session Laws of Hawaii 2004. This report discusses the progress made in complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates, lists all outstanding tasks, and contains an expenditure report (five months actual and seven months projected) of all HIPAA related activities performed by the Department of Human Services (DHS).

I. PROGRESS TOWARDS HIPAA COMPLIANCE

HIPAA is a federal law that focuses on protecting health insurance coverage for workers and their families when they change or lose their jobs (portability), and protecting health information and data integrity, confidentiality, and availability (accountability). HIPAA rules affect the DHS in three ways, by specifying: 1) Privacy of individually identifiable health information; 2) Transaction and Code Set requirements; and 3) Security of individually identifiable health information maintained, sent and/or received electronically. The DHS must comply with HIPAA because it is the State's Medicaid agency.

A. Compliance with the Privacy Rule

The deadline for compliance with the HIPAA Privacy Rule was April 14, 2003. Prior to the deadline, the DHS determined that we are a Hybrid Covered Entity with our covered components being: the Med-QUEST Division ("MQD"), the Medicaid Waiver programs of the Social Services Division ("SSD"), and the Director's Office. With the assistance of consultants, FourThought Group, Inc. out of Phoenix, Arizona, and the Attorney General's office, we were able to draft and implement Department-level Privacy Policies which are part of the DHS' Policies and Procedures Manual. The MQD, the covered components of the SSD, and the Director's Office drafted desktop policies and procedures to assure compliance with the HIPAA Privacy Rule and the Departmental Privacy Policies. MQD and SSD created and distributed their Notice of Privacy Practices to all of their existing clients (approximately 100,000), and created procedures for ongoing distribution to new clients. They also created new forms (including HIPAA compliant authorization forms) to ensure that their clients' privacy rights will be appropriately protected. Once the Department-level and Division-level policies and procedures were implemented, the DHS conducted live training (again with the assistance of FourThought Group) for all employees of its covered components, including all of those on the Neighbor Islands, as required by HIPAA, prior to April 14th, 2003. The DHS Privacy Policies and the Notices of Privacy Practices can be found on the internet at www.hawaii.gov/dhs/, along with a brief summary of the DHS' HIPAA status and the contact information for our Privacy Officer.

Once the DHS met the Privacy Rule deadline, we did not stop there. The DHS had FourThought Group create a computer-based training program in PowerPoint for all new hires or staff transferring from a non-covered component to a covered one. We provided HIPAA training for many employees of our non-covered components, to inform them of the possible difficulties they may face when trying to get information from covered entities, such as doctors and psychologists, and how to overcome them. We also received from FourThought Group the tools to conduct Post-Implementation HIPAA Privacy Rule Compliance Audits within all of our covered components. The contract with FourThought Group was extended from July 31, 2003 to January 31, 2004 to provide needed time necessary to complete all of the deliverables that the DHS requested of them per the contract.

1. The DHS Privacy Officer

The Privacy Officer, who is also the DHS HIPAA Project Director, and assigned staff in SSD and MQD, have been available to answer HIPAA questions asked by other staff members and clients. They also have handled concerns voiced by clients and they have satisfied requests for information and clarified misunderstandings about what HIPAA requires. To date, there have been no formal complaints against the DHS lodged with the DHS Privacy Officer or filed with the U.S. Department of Health and Human Services, Office for Civil Rights.

The Privacy Officer and assigned staff in MQD and SSD participate in the HIPAA Readiness Collaborative ("HRC") of the Hawaii Health Information Corporation and attend Privacy and Security sub-committee meetings. The Privacy Officer was appointed co-chair of the Privacy sub-committee this year. The HRC is made up of most of the major hospitals in the State, HMSA, Kaiser, and smaller medical groups and providers. There are six State Departments that are members of the HRC. The Departments are the DHS, the Department of Health ("DOH"), the Hawai'i Employer-Union Health Benefits Trust Fund, the Department of Public Safety, the Department of Education and the Department of the Attorney General. The Privacy Officers of the DHS and the DOH represent the State on the HRC Steering Committee.

The DHS Privacy Officer participates in monthly meetings of the State HIPAA Contacts Committee which is made up of representatives of the HRC member Departments, to discuss compliance efforts and other issues that arise. It is hoped that this regular communication will bring some consistency in the State's approach to complying with HIPAA.

The DHS Privacy Officer monitors national HIPAA issues and concerns via a national email listserve and website called HIPAAGives, which consists of governmental entities from every state. Members of HIPAAGives sent a letter in May to the DHHS Office for Civil Rights requesting clarification and/or

Privacy Rule changes to the way HIPAA affects Child and Adult Protective Services. To date, HIPAAGives has not received a reply.

B. Transactions and Code Sets

DHS has made consistent and timely efforts to comply with HIPAA Transactions and Code Sets ("TCS") requirements. The deadline for compliance with those requirements was October 16, 2003, and that deadline was met. The TCS rule mandates standards for eight (8) electronic transactions and for code sets. The DHS successfully
implemented the following transactions for the October 2003 TCS implementations:

- ? 837 Fee for Service Claims
- ? 835 Electronic Remittance Advice
- ? 270/271 Eligibility Verification Request and Response
- ? 276/277 Claim Status Request and Response
- ? 834 Health Plan Roster
- ? 820 Premium Payment

The DHS is able to accept and process all of the above transactions through our Hawaii Prepaid Medical Management – Information System (HPMMIS), the Medicaid claims system that exists in partnership with the State of Arizona's Medicaid claim system. The DHS successfully converted most of the local codes to HIPAA compliant codes on October 16, 2003. The DHS will convert the remaining local codes as instructed by Medicare. In October 2003, we notified all affected providers of the local codes change.

The DHS will continue to implement TCS transactions as mandated by federal law. The next major implementation will be for Claims Attachments. For further information about the DHS' implementation of the HIPAA TCS rule, please go to the Med-QUEST Division's website at www.med-quest.us/HIPAA.

C. Compliance with the Security Rule

The HIPAA Security Rule was finalized on February 20, 2003. The Security Rule sets forth standards for the administrative, physical, and technological safeguards on individual health data stored in an electronic form. It specifies the minimum requirements and implementation specifications that a covered entity such as the DHS must maintain in order to ensure the confidentiality, integrity and availability of the individual health data it has in its possession. The requirements apply to data that is housed on mainframe computers and network servers, as well as the storing, sharing, copying, transmitting and disposing of such data.

Within DHS' first contract with FourThought Group, Inc., the consultants were able to conduct an assessment of the DHS' systems and networks from a Security Rule perspective. FourThought Group was able to subcontract with a local company, Secure Technology Hawaii, Inc. to conduct on-sight interviews,

systems scans, and wardialing of DHS telephone lines to determine where possible Security breaches and vulnerabilities might be.

Secure Technology finished this task and sent a report with recommendations to FourThought Group. FourThought Group incorporated this information into a final report which the DHS received on February 5, 2004. The report included: an analysis of internal and external electronic information flows; an analysis of network hardware and software inventories and application interfaces; documentation and analysis of HIPAA security gaps, security threats, and network and system vulnerabilities; an analysis of new network architecture being proposed by our Benefit, Employment, and Support Services Division vis á vis the Security Rule; and detailed recommendations which included identification of potential technical solutions. The report also included the steps needed to complete a Risk Analysis, a Risk Management Plan, and a Contingency Plan.

The deadline for complying with the Security Rule is April 20, 2005. By this date, the DHS must have in place the policies, procedures, and the physical and technological safeguards that meet the requirements of the rule, or face federal financial penalties and possible civil lawsuits. The DHS will need to complete the Risk Analysis, the Risk Management Plan, and the Contingency Plan, as well as to implement the changes required by the Security Rule as recommended by FourThought Group. The DHS has been able to contract with FourThought Group again to provide assistance to implement these safeguards to satisfy the Security Rule requirements. Pursuant to Security Rule requirements the DHS has designated its HIPAA Project Director as its Information Security Officer to oversee, not only the creation and enforcement of the HIPAA Security Policies and Procedures, but also the Risk Management Plan and the Contingency Plan and, of course, the contract with FourThought Group, Inc.

II. POSSIBLE PENALTIES FOR NON-COMPLIANCE

The U.S. Department of Justice is enforcing three types of HIPAA violations that are considered to be criminal in nature. For "Wrongful Disclosure" there are fines of up to $50,000 or up to one year imprisonment for each offense. For "False Pretense" there are fines of up to $100,000 or up to 10 years imprisonment for each offense. For "Intent to Sell, Transfer or Use" for commercial advantage, personal gain or malicious harm, the penalties are up to $250,000 or up to 10 years imprisonment for each offense. The U.S. Department of Health and Human Services, Office for Civil Rights, is enforcing the civil violations of the HIPAA regulations. They are empowered to issue fines for civil HIPAA violations of up to $100 per incident, and up to $25,000 per person, per year, per standard.

There is also concern for civil liability among the Covered Entities in Hawai'i, that despite the fact that there is no State cause of action for violations of HIPAA, Hawai'i does have a Right to Privacy in its Constitution. Potential plaintiffs could

bring a lawsuit against a Covered Entity alleging that it violated the plaintiff's right to privacy by violating HIPAA, which is considered a national standard.

III. EXPENDITURE REPORT

Last Legislative session, the DHS' MQD received $250,000 in general funds which will be matched with approximately $2,250,000 in federal funds, to assist the DHS to comply with the HIPAA Security Rule as it pertains to information technology hardware, software and consulting services. The DHS has just contracted with FourThought Group, Inc., again, to assist with its Security Rule implementation and maintenance initiatives. That contract, in two phases, will go from November 8, 2004 until June 30, 2006, at a cost of $218,004.00 in general funds to be matched by $1,572,396.00 in federal funds, at a federal match of nearly 90%. The remaining $7,807.20 in general funds will be used, at a blended federal match of approximately 75%, to further upgrade systems, networks, and desktops as determined by the DHS' Security Risk Management Plan and Business Contingency Plan.