

**SERVICES AND ENTERPRISE SUPPORT
ADMINISTRATION**



Confidential Data Compliance with HIPAA

Request	FY16	FY17	15-17
FTE	3.0	3.0	3.0
GF-State	\$714,000	\$714,000	\$1,428,000
Total	\$871,000	\$871,000	\$1,742,000

DECISION PACKAGE SUMMARY

The Services and Enterprise Support Administration (SESA) requests funding for staff and training in order to comply with newly adopted federal privacy rules. By funding this request, the department is expected to achieve compliance with the significant changes to the Health Information Portability and Accountability Act brought about by newly adopted Omnibus Rules.

PROBLEM STATEMENT

DSHS must comply with and monitor adherence to Health Information Portability and Accountability Act (HIPAA) Omnibus Rules. Updated rules took effect September 23, 2013 and require significant and ongoing changes to agency policies and practice. These changes are important to avoiding security breaches and potential fines from the Department of Health and Human Services Office of Civil Rights (OCR). Expectations for DSHS from HIPAA and other privacy rules require additional staff resources including a full time privacy officer, a manager to oversee application of the security rules, and a position that develops and implements training for staff on HIPAA. Not only does DSHS need to change policy and practice, but compliance with these changes must be assessed, documented, and re-assessed at least every two years. The requested staff will ensure that the agency’s practices remain aligned with HIPAA rules.

DSHS serves over 2 million clients per year, has over 17,000 employees, and holds over 80,000 contracts. HIPAA and other confidentiality laws apply to all parts of DSHS, and compliance to new rules will not be achieved without new resources. In the absence of the requested resources DSHS is at substantial risk to have a breach of confidential records and/or Protected Health Information (PHI). The department can receive significant financial penalties from OCR for any breaches of confidentiality. Examples of recent OCR fines of public entities include a \$1.7 million fine to the State of Alaska, \$400,000 fine to Idaho State University, and \$215,000 fine to Skagit County Department of Health. All fines were for loss of unsecured protected health information due to a lack of compliance to HIPAA Privacy and Security Rules.



DSHS VISION
People are healthy • People are safe • People are supported • Taxpayer resources are guarded

DSHS MISSION
To transform lives

DSHS VALUES
Honesty and Integrity • Pursuit of Excellence • Open Communication • Diversity and Inclusion • Commitment to Service

SESA

Confidential Data Compliance with HIPAA



2015-17 BIENNIAL BUDGET

PROPOSED SOLUTION

Needed resources include 1.0 FTE to function as the DSHS Privacy Officer, 1.0 FTE for assessing agency compliance with the security rules, and 1.0 FTE for specific training development and delivery of training in DSHS. In addition, the agency requests backfill for direct care staff in DSHS who need to be trained in the new requirements. The requested resources are the minimum amount needed to support broader compliance with privacy rules throughout the department. Implementation of the rules began September 23, 2013 but the requirements include ongoing improvements and monitoring of agency compliance.

EXPECTED RESULTS

The budget request supports DSHS Goal 5: Public Trust – Strong management practices will be used to ensure quality and efficiency. The decision package is essential to implementing the SESA's Strategic Objective 5.6: Through department-wide processes and policy, ensure that strong procedures are in place for the protection of DSHS clients' information and records. This request also supports the Results Washington goal to have Effective, Efficient and Accountable Government.

DSHS holds large volumes of confidential client data, which must be protected from unauthorized release and breaches in confidentiality laws and rules. Last year DSHS reported 41 breaches to the OCR. In each one of these breaches, confidential client information was available to individuals that did not have a right to see the information. DSHS has well over 200 information sets that contain confidential client data including PHI. These systems must each have a risk analysis completed to determine whether they comply with HIPAA and other confidentiality laws. In addition, DSHS must implement corrective action plans as well as update and revise policy and practice to comply with federal and state laws governing confidential information. DSHS aims to reduce reportable breaches to OCR by 50% in the coming year. This request is essential to accomplishing this goal as well as reducing DSHS vulnerability for fines levied by the federal government. Any unauthorized data release could potentially place the welfare of clients in jeopardy.

STAKEHOLDER IMPACT

DSHS stakeholders, partners, and clients are unlikely to have concerns about the proposed investment since compliance with HIPAA and other privacy laws and rules benefits each of these parties.



DSHS VISION

People are healthy • People are safe • People are supported • Taxpayer resources are guarded

DSHS MISSION

To transform lives

DSHS VALUES

Honesty and Integrity • Pursuit of Excellence • Open Communication • Diversity and Inclusion • Commitment to Service