4002 DHS PRIVACY AND SECURITY SANCTIONS

I. Authority

This policy implements the mandated sanction guidelines of HIPAA (Health Insurance Portability and Accountability Act), FISMA (Federal Information Security Management Act), the Arkansas Crime Information Center (ACIC) and the National Crime Information Center (NCIC). This policy protects and secures all DHS client and patient information as mandated by HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, the State of Arkansas' Personal Information Protection Act (PIPA), ACIC, NCIC, Arkansas law protecting foster care and protective services information (Ark. Code Ann. § 9-28-407(h)) and all other federal laws and rules and regulations.

II. Compliance

(a) The meaning and intent of this policy is for all DHS employees to maintain compliance with all applicable federal and state laws, acts, and regulations governing the protection of sensitive and confidential data including, but not limited to, Protected Health Information (PHI), Personal Identifying Information (PII), Federal Tax Information (FTI), Social Security Information, and all client or patient information considered confidential. This policy ensures that all DHS employees will be held to the same standards and will face the same sanctions for privacy and security violations.

(b) The Standards for Privacy of Individually Identifiable Health Information (the HIPAA Privacy Rule) mandates that DHS must have a policy that applies appropriate sanctions against workforce members who violate privacy policies and procedures or the Privacy Rule. The U.S. Department of Health and Human Services, Office for Civil Rights is responsible for administering and enforcing these standards and may conduct complaint investigations and compliance reviews. Failing to comply voluntarily with the standards may result in civil money penalties. In addition, certain violations of the Privacy Rule may be subject to criminal prosecution.

III. Applicability

(a) Because of the impact privacy and security violations can have against DHS as an agency, and because such violations can generate fines and can now be considered criminal on an individual basis, this sanctions policy supersedes any other agency policy should conflicts arise.

(b) Any appeal of sanctions from this policy will be governed by DHS Policy 1086, "Employee Grievance/Mediation Policy Dispute Resolution Rules and Procedures." However, those hearing such appeals, both inside and outside the agency, must consider that some sanction(s) given to employees are based on federal regulations and reported to federal authorities as mandated by law (Refer to Section II (b) "Compliance"). Any change or repeal of sanctioning could

cause an inconsistency among the same offenses which may result in fines to the agency.

(c) DHS is a hybrid entity in that it is a covered entity whose business activities include both covered and non-covered functions and contains designated health care components in accordance with HIPAA. This sanctions policy enforces the protection of all confidential information and is applicable to all DHS employees, regardless of the division in which they work. All DHS employees will be responsible and held accountable per this policy for any and all confidential information they handle in the course of their employment.

IV. Definitions

(a) Breach: Any impermissible use or disclosure of confidential information or Protected Health Information (PHI).

(b) Business Associate, Covered Entity, Hybrid Entity: As defined by HIPAA Definitions (45 C.F.R. §§160.103, 164.103).

(c) Chief Information Security Officer: DHS official who is responsible for the security of all information systems, oversees all investigations into security incidents, and may recommend consistent and appropriate sanctions against DHS employees for security violations.

(d) Confidential Information: Information that must be protected from disclosure by a federal or state law, rule, or regulation, including without limitation Protected Health Information (PHI) and Personal Identifying Information (PII), such as Social Security Numbers, foster children's information, or client IP addresses.

(e) Contractor: An individual or company/vendor under contract with DHS who must sign a Business Associate Agreement. The HIPAA Omnibus Rule subjects Business Associates to the same liabilities as a Covered Entity.

(f) DHS Incident Reporting System: Located on DHS Share, the system DHS employees must use to report privacy or security incidents, including suspected incidents.

(g) Personal Identifying Information (PII): Any information about an individual maintained by an agency and that is protected from disclosure by a federal or state law, rule, or regulation, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

(h) Privacy Incident: A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access to confidential information,

including but not limited to, Personal Identifying Information (PII) and Protected Health Information (PHI).

(i) Privacy Officer: A DHS official (required by HIPAA) who is responsible for developing and implementing privacy policies and procedures, reports breaches of PHI to federal authorities, and recommends consistent and appropriate sanctions against DHS employees for privacy violations.

(j) Privacy Office: A DHS contact office (required by HIPAA) responsible for receiving privacy complaints, investigating privacy incidents, and providing clients with information and DHS employees with training on privacy practices.

(k) Protected Health Information (PHI): Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

(l) Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

V. Policy

(a) All privacy or security incidents, even suspected incidents, must be reported immediately by all DHS employees, contractors, and vendors by utilizing the DHS Incident Reporting System located on DHS Share. Examples of incidents include, but are not limited to:

(1) Lost, missing, or stolen electronic devices, (laptops, i-Pads, tablets, cell phones, cameras, flash drives--whether encrypted or not, the loss of these items must be reported);

(2) Lost, missing, or stolen files or documents containing confidential information of DHS clients or employees;

(3) Confidential information e-mailed, post mailed, or faxed to wrong recipient;

(4) Failure to e-mail confidential information outside of DHS with "SENSITIVE" in the subject line; or,

(5) Any incident in which an unauthorized person obtains or views confidential information.

(b) Reporting a privacy or security incident to a supervisor is not sufficient to comply with the reporting requirement. If an employee reports an incident to a supervisor, it becomes both the employee's and the supervisor's responsibility to ensure that the incident is immediately reported to the DHS Privacy Office via the Incident Reporting System. Any questions can be directed to the DHS Privacy Office.

(c) If an employee with the DHS Privacy Office instructs a DHS employee or supervisor to file a report via the Incident Reporting System and the employee fails to do so, that will be considered a Failure to Report Class II Offense and subject to a Class II Sanction.

(d) Determination of the status of an incident as a reportable breach or a non-reportable breach to the United States Health and Human Services Secretary or other state or federal agencies will be made by the DHS Privacy Officer following the report and a full investigation of the occurrence.

(e) The DHS Privacy Office or the Information Security Unit will diligently attempt to complete an investigation within 30 days of receiving an incident report. However, the timelines in policy 1084 do not apply to discipline administered under this policy because those timelines were established without consideration of the additional time required to investigate, mitigate, and resolve privacy or security incidents and breaches, and investigations following this policy are federally mandated and must follow federal protocols.

VI. Offenses

(a) Examples of Class I Offenses include, without limitation:

(1) Accessing confidential information you do not need to know to do your job;

(2) Sharing your computer access codes (user name and password, or password alone);

(3) Leaving your computer unattended while you are logged into a system containing confidential information (for example, MMIS or CHRIS);

(4) Losing an agency-issued electronic device (laptop, cell phone, etc.) or agency files containing client or patient confidential information;

(5) Sharing confidential information with another employee, contractor, or vendor without authorization;

(6) Copying or recording confidential information without authorization;

(7) Emailing or downloading confidential information without authorization to non-DHS personal electronic devices such as flash drives, home computers, or mobile devices;

(8) Changing confidential information without authorization;

(9) Discussing confidential information in a public area or in an area where the public could overhear the conversation;

(10) Discussing confidential information with an unauthorized person;

(11) Failing to report actual or suspected privacy or security incidences regarding the loss or misuse of confidential information; or,

(12) Failing to comply with a DHS Privacy or Security Policy, (DHS Policies 1001-1003, 4000s-5000s), depending on the severity of the violation (See Section VII. "Determination of Sanctions").

(b) Class II Offenses

(1) Second offense of any Class I offense (does not have to be the same offense and can occur within the same incident);

(2) Using or disclosing confidential information without authorization;

(3) Using another person's computer access codes (user name & password) (this does not include IT staff conducting an authorized investigation);

(4) Losing an agency-issued electronic device (laptop, cell phone, etc.) or agency files containing client or patient confidential information, as a result of negligence or reckless disregard of DHS policies;

(5) Failing to cooperate with the DHS Privacy Officer or the Chief Information Security Officer during the course of an investigation;

(6) Failing to comply with a resolution, team resolution, or recommendation from the agency Privacy Office or the Chief Information Security Officer that is approved by the Director of the Office of Policy and Legal Services;

(7) Failing to report a privacy or security incident after being instructed to do so by an employee with the DHS Privacy Office or with the DHS Information Security unit;

(8) Failing to obtain certification from training mandated by the Privacy or Chief Information Security Officers as a sanction for a violation; or,

(9) Failing to comply with a DHS Privacy or Security Policy, (DHS Policies 1001-1003, 4000s-5000s) depending on the severity of the violation. (See Section VII. "Determination of Sanctions")

(c) Class III Offenses

(1) Third offense of any Class I offense (does not have to be the same offense and can occur within the same incident);

(2) Second offense of any Class II offense (does not have to be the same offense and can occur within the same incident);

(3) The compilation of any two Class I offenses in addition to any one Class II offense (does not have to be the same offense and can occur within the same incident);

(4) Being dishonest, being misleading, or misstating facts to the DHS Privacy Officer, the Chief Information Security Officer, or their staff during the course of an investigation;

(5) Obtaining confidential or protected information (such as PHI) under false pretenses;

(6) Bypassing willfully or intentionally any DHS security controls (such as plugging in an unsecured wireless access point with no protections, placing key loggers on computers, using someone else's smartcard); or,

(7) Using or disclosing confidential information for commercial advantage, personal gain or malicious harm.

VII. Sanctions

(a) Class I Sanctions can include one or more of the following:

(1) Written reprimand in employee's personnel file;

(2) Retraining and recertification on the DHS Privacy and Security Policy, if the offense was a security violation; or

(3) Training and certification on HIPAA Awareness, if the offense was a Privacy offense.

(b) Class II Sanctions can include one or both of the following:

(1) Written reprimand in employee's personnel file as well as retraining in DHS Privacy and Security policy or HIPAA Awareness;

(2) Suspension of employee (minimum of one (1) day and maximum of three (3) days).

(c) Class III Sanctions can include one or more of the following:

(1) Termination of employment;

(2) Termination of contract;

(3) Civil penalties as provided under HIPAA or other applicable Federal, State, or Local law; or,

(4) Criminal penalties as provided under HIPAA or other applicable Federal, State, or Local law.

VIII. Determination of Sanctions

(a) The DHS Privacy Officer, the employee's Division Director or designee (i.e., someone from the employee's supervisory chain authorized to process disciplinary action), and the DHS Chief Information Security Officer shall determine whether an employee shall be:

(1) Suspended from duty with full pay and benefits pending investigation; or,

(2) Disciplined, and if so, the level of discipline to be administered. (An attorney from the Office of Chief Counsel shall be consulted prior to any termination or suspension without pay.)

(b) If the group listed in Section VIII (a) above cannot come to an agreement regarding the sanction, then the Director or Chief Attorney of the Office of Chief Counsel will make the final determination.

(c) Disciplinary determinations shall consider the seriousness of the loss of information, the financial impact on the agency, the employee's culpability, and the civil money penalty criteria in 45 C.F.R. § 160.408.

(d) A single privacy or security incident could include more than one offense. For example, if an employee is involved in an incident in which he or she commits three Class I Offenses, then the employee would face a Class III Sanction.

(e) The employee's supervisor will administer the disciplinary action as determined by the group listed in Section VIII (a) of this policy. If the employee's supervisor is not authorized to discipline the employee, then a person with disciplinary authority over the employee will process the recommended disciplinary action.

(f) The employee's supervisor may request that the DHS Privacy Officer assist with discussing the investigation and findings with the employee. The supervisor will present the employee with the approved sanction and outline the disciplinary action on a DHS-1173, "Notice of Disciplinary Action" form. If the employee refuses to sign the DHS-1173, a supervisor or other management staff shall witness the refusal and note it on the document.

(g) Whether reportable to federal authorities or law enforcement or not, the following factors will be considered by the group listed in Section VIII (a) when determining sanctions:

(1) The nature and extent of the violation, specifically, the number of individuals affected and the time period during which the violation occurred, (if confidential information is involved, note the state or federal law or rule that identifies the information as confidential);

(2) The nature and extent of the harm resulting from the violation, specifically, whether the violation caused physical harm, financial harm, harm to DHS or an individual's reputation, or hindered an individual's ability to obtain health care;

(3) The nature and extent of the protected information involved, that is, consider the types of identifiers and likelihood of re-identification, the unauthorized person who used the protected information or to whom the disclosure was made; whether the protected information was actually acquired or viewed; and, the extent to which the risk to the protected information has been mitigated;

(4) The history of prior compliance, whether the current violation is the same or similar to previous indications of noncompliance, to what extent the employee has attempted to correct previous indications of noncompliance, how the employee has responded to technical assistance from the DHS Privacy Office and the Information Security Unit in the context of a compliance effort or investigation, and how the employee has responded to prior complaints;

(5) Damages to property, security controls, and such other matters as justice may require.

IX. Ineligible for Re-hire

Employees discharged for violations of this policy are permanently disqualified from re-hire because they endangered the confidentiality of information of agency clients or patients and by doing so jeopardized the integrity of DHS.

X. Clarification

(a) This sanctions policy does not prohibit applying other sanctions from DHS Policy, including DHS Policy 1084, to the same disciplinary action. The employee's supervisor(s) may need to include other applicable DHS policy violations to the disciplinary action regarding the privacy or security violation. This could result in action up to and including termination and prosecution. Supervisors may contact the DHS Office of Policy and Legal Services with any questions on how to proceed.

(b) This policy does not alter the employment-at-will doctrine.

(c) Failure to follow any aspect of this policy may be considered a failure to comply (under DHS Policy 1084) which shall result in disciplinary action.