4002 DHS PRIVACY AND SECURITY SANCTIONS

I. Authority

This policy implements the mandated sanction guidelines of Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), the Arkansas Crime Information Center (ACIC), and the National Crime Information Center (NCIC). This policy protects and secures all Department of Human Services (DHS) client and patient information as mandated by HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, the State of Arkansas's 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. Definitions

(A) Breach: any impermissible use or impermissible disclosure of confidential information or Protected Health Information (PHI) whether intentional or accidental.

(B) Business Associate, Covered Entity, Hybrid Entity: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. It includes a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. As defined by HIPAA Definitions (45 C.F.R. §§160.103, 164.103).

(C) Business Associate Agreement: an agreement that ensures that the business associate will appropriately safeguard protected health information. It also clarifies and limits, as appropriate, the permissible uses and disclosures of protected health information by the business associate.

(D) Chief Information Security Officer (CISO): DHS official who maintains the security of all information systems, oversees all investigations into security incidents, and recommends consistent and appropriate sanctions against DHS employees for security violations.

(E) 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), Personal Identifying Information (PII), such as Social Security Numbers, foster children's information, or client IP addresses.

(F) 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.

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

(H) HIPAA Omnibus Rule: a HIPAA rule that implemented a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, added further requirements for data breach notifications and penalty enforcements, and subjected business associates and subcontractors to the same rules as a Covered Entity.

(I) 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.

(J) 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).

(K) Privacy Officer: a DHS official (required by HIPAA) who develops and implements privacy policies and procedures, reports breaches of PHI to federal authorities, and recommends consistent and appropriate sanctions against DHS employees for privacy violations.

(L) 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.

(M) 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.

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

III. Compliance

(A) The intent of this policy is for all DHS employees to comply with all applicable federal and state laws, acts, and regulations governing the protection of confidential data including, but not limited to, PHI, 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.

(C) DHS is a hybrid entity in that its 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. All DHS employees will be held accountable per this policy for any and all confidential information they handle in the course of their employment.

IV. Policy

(A) All privacy or security incidents, even suspected incidents, must be reported immediately by all DHS employees, contractors, and vendors by using 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, whether encrypted or not (laptops/computers, tablets, cell phones, cameras, flash drives, recorders, 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 an offense and the employee may be sanctioned.

(D) The DHS Privacy Officer will conduct an investigation and determine if an incident is a reportable breach within the required timeframe.

V. Offenses

(A) Pursuant to 45 CFR § 164.530, DHS must have and apply appropriate sanctions against employees who fail to comply with DHS privacy policies and procedures. Examples of privacy offenses which may result in sanctions include, without limitation:

(1) Accessing confidential information not needed to do the job;

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

(3) Leaving a computer unattended while 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, downloading, uploading, or sharing of confidential information without CISO authorization to non-DHS email accounts or 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;

(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”);

(13) Using or disclosing confidential information without authorization;

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

(15) Failing to cooperate with the DHS Privacy Officer or the CISO during the course of an investigation;

(16) Failing to comply with a resolution, team resolution, or recommendation from the agency Privacy Office or the CISO that is approved by the Director of the Office of Chief Counsel;

(17) 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 Office of Information Technology (OIT);

(18) Failing to obtain certification from training mandated by the Privacy or CISO as a sanction for a violation;

(19) Failing to comply with a DHS Privacy or Security Policy, (DHS Policies 1001-1003, 4000s-5000s) depending on the severity of the violation.

(20) Being dishonest, being misleading, or misstating facts to the DHS Privacy Officer, the CISO, or their staff during the course of an investigation;

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

(22) 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,

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

VI. Sanctions

The DHS Privacy Officer, the employee's Division Director, Office Chief, or designee, and the DHS CISO shall determine the appropriate level of sanctions for an employee that violates DHS privacy policies and procedures. If they cannot come to an agreement regarding the sanction, then the DHS Secretary or Chief Counsel will make the final determination.

(A) The following factors will be considered by the DHS Privacy Officer, the employee's Division Director, Office Chief, or designee, and the DHS CISO 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 considering 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 incidents of noncompliance, how the employee has responded to technical assistance from the DHS Privacy Office and the OIT in the context of a compliance effort or investigation, and how the employee has responded to prior complaints; and

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

(B) Sanctions for a failure to comply with DHS privacy policies and procedures may 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;

(3) Training and certification on HIPAA Awareness, if the offense was a privacy offense;

(4) Suspension of employee (An attorney from the Office of Chief Counsel shall be consulted prior to suspension);

(5) Termination of employment (An attorney from the Office of Chief Counsel shall be consulted prior to any termination);

(6) Termination of contract (If there is a conflict between this policy and the terms of a contract, the contract terms are controlling);

(7) Civil penalties as provided under HIPAA or other applicable Federal, State, or local law; and/or,

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

Note: An attorney from the Office of Chief Counsel shall be consulted prior to any termination or suspension without pay.

(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 supervisor will administer the disciplinary action associated with this policy.

(E) The 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.

(F) Any appeal of sanctions from this policy will be governed by DHS Policy 1086, "Employee Grievance and Mediation Policy." However, those appeals, both inside and outside the agency, must consider that some sanction(s) are based on federal regulations and reported to federal authorities as mandated by law (Refer to Section III (B) "Compliance"). Any change or repeal of sanctioning could cause an inconsistency among the same offenses which may result in fines to the agency.

VII. Clarification

This sanctions policy does not prohibit applying additional sanctions from DHS Policy, including DHS Policy 1084, to the same disciplinary action.