ARIZONA DEPARTMENT OF CHILD SAFETY

TITLE	POLICY NUMBER	
HIPAA Privacy	DCS 07-16	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
Audit Management Services	11/26/18	3

I. POLICY STATEMENT

The Health Insurance Portability and Accountability Act (HIPAA) establishes national privacy standards for safeguarding health care information. HIPAA's standards for privacy of protected health information (PHI), also referred to as the "Privacy Rule", address the use and disclosure of individuals' PHI, as well as individuals' rights to understand and control how their health information is used.

The Department of Child Safety (DCS) designates itself as a "covered entity" under HIPAA, and is therefore subject to the Privacy Rule. DCS is committed to the zealous protection of PHI. The Department shall adopt and implement the standards, requirements, and implementation specifications of HIPAA's Privacy Rule with respect to Protected Health Information [HIPAA 45 CFR Part 164, Subpart E – Privacy of Individually Identifiable Health Information].

II. APPLICABILITY

The standards, requirements, and implementation specifications of HIPAA's Privacy Rule apply to the DCS workforce, business associates, and PHI transmitted or maintained in any form or medium. Related DCS Information Technology policies that address data integrity include DCS 05-8120 (Information Security Program), DCS 05-8250 (Media Protection), and DCS 05-8260 (Physical Security Protections).

III. AUTHORITY

Public Law 104-191 Health Insurance Privacy and Portability Act

45 CFR Subtitle A, Subchapter C, Parts 160, 162, and 164

IV. DEFINITIONS

Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA [HIPAA 45 CFR § 164.402].

Business Associate: An entity or person who performs a function involving the use or disclosure of PHI on behalf of a covered entity (e.g. claims processing, case management, utilization review, quality assurance, billing) or provides services for a covered entity that require the disclosure of PHI (e.g. legal, actuarial, accounting, accreditation) [HIPAA 45 CFR § 160.103].

Code of Federal Regulations (CFR): An annual codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the U.S. Government.

Covered Entity: A health plan, a health clearinghouse, or a health care provider who transmits any health information in electronic form in connection to a transaction covered by HIPAA [HIPAA 45 CFR § 160.103].

Data Incident: Includes the loss of control, compromise, "accidental disclosure" such as misdirected e-mails or faxes, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any term referring to situations where persons other than authorized users, and for other than an authorized purpose, have access or potential access to unencrypted, unprotected, or unredacted confidential information, whether physical or electronic.

Department or DCS: The Arizona Department of Child Safety.

Disclosure: The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information [HIPAA 45 CFR § 160.103].

Electronic Protected Heath Information (ePHI): Protected health information (PHI) in electronic form.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): Federal legislation that establishes privacy and security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers.

HIPAA Privacy Rule: Establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. It requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. It also gives patients' rights over their health information, including the right to examine and obtain a copy of their health records, and to request corrections.

Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and:

- is created or received by a health care provider, health plan, employer, or health care clearinghouse;
- relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual [HIPAA 45 CFR § 160.103].

Least Privilege: The principle that allows authorized access for users (or processes acting on behalf of users) necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Limited Data Set: Protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set [HIPAA Privacy Rule, Permitted Uses and Disclosures, (6)].

Minimum Necessary Standard: The concept that reasonable efforts shall be made to limit PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request [HIPAA 45 CFR 164.502 (b)].

Protected Health Information (PHI): Individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Individually identifiable health information excludes health information in education records covered by the Family Educational Rights and Privacy Act or in employment records held by a covered entity in its role as employer [HIPAA 45 CFR § 160.103].

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether they are paid by the covered entity or business associate.

V. POLICY

A. Uses and Disclosure of PHI

DCS assures the privacy and confidentiality of PHI. Members of the DCS workforce shall not permit the unauthorized disclosure of PHI except as *permitted* or *required* by law.

1. DCS is *permitted* to disclose PHI as follows:

   a. to the applicable individual;

   b. for treatment, payment, or health care operations;

   c. for uses after the individual is notified and given the opportunity to object to the use or disclosure;

   d. incident to a use or disclosure otherwise permitted or required by law;

   e. for public interest and benefit activities;

   f. as a limited data set for the purpose of research, public health, or health care operations.

   DCS shall rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

2. DCS is *required* to disclose PHI:

   a. to the applicable individual or individual's designee, as necessary to satisfy an individual's request for an electronic copy of PHI;

   b. when required by the Secretary of Health and Human Services to investigate or determine the Department’s compliance with this act.

DCS shall employ the concept of *least privilege*, allowing only authorized accesses to PHI.

DCS shall mitigate, to the extent practicable, any harmful effect that is known as a result of a use or disclosure of PHI in violation of these policies and procedures by DCS or any of its business associates.

B. Training

DCS shall train workforce members on HIPAA as necessary and appropriate for them to carry out their functions. (Business Associates train their workforce on the HIPAA Rule and keep appropriate records of training as prescribed in HIPAA 45 CFR 164.530 (b) (1) (2)). DCS shall provide initial and ongoing security awareness training programs for all members of its workforce (including management). See DCS Policy 05-8210, Security Awareness Training and Education.

C. Privacy Requirements for Contractors and Service Providers

DCS may disclose PHI to a business associate and may allow that associate to create, receive, maintain, or transmit PHI on its behalf. DCS shall establish privacy requirements in contracts with business associates that perform covered functions, including the permitted and required uses and disclosures of PHI by the business associate. Contracts may permit the business associate to use and disclose PHI for the proper management and administration of the business associate and not use or further disclose the information other than as permitted or required by the contract or as required by law.

D. Minimum Necessary Standard

When collecting, using, or disclosing PHI, or when requesting PHI from another covered entity or business associate, DCS shall observe the *minimum necessary standard*. PHI shall not be used or disclosed when it is not necessary to satisfy a particular purpose or function.

In order to comply with the minimum necessary standard, DCS shall periodically evaluate its practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI.

The minimum necessary rule is not required to be applied under the following circumstances:

- for treatment;
- for disclosure to the individual who is the subject of the information, or the individual's personal representative;
- in accordance with the applicable individual's valid authorization;
- to the Office of Civil Rights for HIPAA complaint investigation, compliance review, or enforcement purposes;
- as required by law; and
- as required for compliance with HIPAA rules.

E. DCS Privacy Officer Responsibilities

The DCS Privacy Officer shall:

1. Assist the Field Resources and Policy Unit in the development, implementation, maintenance, and, as necessary, periodic revision of this policy;

2. Track, document, investigate, and resolve all privacy matters.

F. Data Safeguards

DCS shall ensure the confidentiality, integrity, and availability of all PHI it creates, receives, maintains, or transmits. DCS shall maintain appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure that is unauthorized and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. These safeguards are established in several DCS policies including Information Security Program (DCS 05-8120), Security System Maintenance (DCS 05-8220), Media Protection (DCS 05-8250), Physical Security Protections (DCS 05-8260), Personnel Security Protection (DCS 05-8270), Acceptable Use (DCS 05-8280), Access Control (DCS 05-8320), Identification and Authorization (DCS 05-8340), and System and Communications Protection (DCS 05-8350).

G. Complaint Management

DCS shall provide a process for individuals to make complaints related to PHI. The *Notice of Privacy Practices*, required per 45 CFR § 164.520(a)-(b), shall include information regarding whom to contact with complaints, concerns, or questions about privacy practices. Complainants may file an Unusual Incident Report form. All complaints received, and their dispositions (if any), shall be documented. DCS has a designated Privacy Officer as the contact person or office

who is responsible for receiving complaints and who is able to provide further information about matters covered by this policy.

H. Documentation and Record Retention

DCS shall maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

DCS shall dispose of, destroy, erase, and/or anonymize PHI, regardless of the method of storage, in accordance with an Arizona State Library, Archives and Public Records approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

VI. PROCEDURES

A. Incident Response Reporting

1. Employee

Immediately after an incident is discovered, but no later than one workday, the employee most closely involved makes a verbal report of the incident to his/her supervisor. This report includes include the following information:

a. person(s) involved in the incident;

b. type of incident i.e. data breach, lost case files, confidential information disclosure;

c. location of the incident;

d. date and time of the incident;

e. witnesses to the incident;

f. description of the incident.

If the incident involves theft, the appropriate law enforcement agency must be notified and a police report will be filed no later than 24 hours after discovery.

For an incident discovered outside employee's normal business hours or workdays, the employee will report the incident to the supervisor the next workday, unless the supervisor is available and on duty.

In the event the supervisor is not available within one workday of incident discovery, the employee will report the incident to another supervisor or his/her supervisor's manager.

NOTE: Incidents that could potentially compromise DCS' information system (e.g. login password disclosure to another person) must be reported directly to Privacy@azdcs.gov immediately.

2. Supervisor

The employee's supervisor or the person who received the report from the employee completes an *Unusual Incident Report* form and distributes it via email within one workday of reporting to OpRiskManagement@azdcs.gov.

For loss or theft of state property, a *Property Loss Report* will also be completed.

3. Contractor

Contractors will report data incidents directly to DCS Privacy Officer.

B. Breach Notification

Upon learning of an impermissible acquisition, access, use, or disclosure of protected health information, a breach will be presumed. The DCS Privacy Officer will begin an investigation and, if appropriate, risk assessment to determine the probability that PHI has been compromised. This investigation shall begin as soon as practical and in no case more than 5 days after learning of the potential breach.

Incident Investigation

Upon notification of the incident, the DCS Privacy Officer will start the investigation and mitigation process.

1. For incidents reported by DCS staff, the DCS Privacy Officer will:

    a. promptly notify Information Technology regarding events that could potentially compromise DCS' information system;

    b. review the Unusual Incident Report form;

    c. contact the employee and /or supervisor for an incomplete submission of the Unusual Incident Report form;

    d. request supporting documentation pertaining to the incident, such as inadvertent communication to an unauthorized user, reproduction of data from a lost case record or stolen laptop, etc. Also request the following:

        i. the number of files, records or persons affected;

        ii. whether the information was recovered, could not be retained or otherwise used or further disclosed by the unauthorized recipient;

        iii. encryption of the data or device affected;

        iv. circumstances that render the information unusable, unreadable, or indecipherable and cannot be re-identified (e.g. redaction).

    e. perform an assessment as to whether or not a breach occurred;

    f. develop a mitigation plan;

    g. perform a risk of harm assessment to determine if affected individuals must be notified. For incidents categorized as breaches under HIPAA, the Privacy Office will submit notification to affected individuals;

    h. identify the number of affected individuals.

2. For incidents reported by a contractor, the DCS Privacy Office will:

a. require the appropriate functional area within DCS to provide the existing agreements between DCS and the contractor;

b. request the contractor to provide specific information about the nature of the incident and individuals affected including:

i. the numbers of files, records, or persons affected;

ii. whether the information was recovered, could not be retained or otherwise used or further disclosed by the unauthorized recipient;

iii. encryption of the data or device affected;

iv. circumstances that render the information unusable, unreadable or indecipherable and cannot be re-identified (e.g. redaction);

v. other assistance to assess risk of harm, plan and implement corrective action.

c. require full collaboration for the mitigation and closure of incidents;

d. request the contractor to provide a written plan explaining steps taken to mitigate the incident and steps taken to avoid reoccurrences.

Notification of individuals:

DCS is designated as a "Covered Entity" under HIPAA, therefore is subject to notification in the case of breach of unsecured protected health information according to 45 C.F.R. §§ 164.400-414.

1. HIPAA Breach Notification for incidents involving DCS employees where the number of affected individuals is less than 500:

a. The DCS Privacy Office will send written notice by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. Written notice shall be provided no later than 60 calendar days after discovery of a breach;

b. If the individual is deceased and the address of the next of kin or personal representative of the individual is known, a written notification by first-class mail will be sent to either the next of kin or personal representative of the individual. However, a written notification will not be sent to the next of kin or personal representative of the individual when the contact information is insufficient or out-of-date that precludes written notification to the next of kin or personal representative of the individual;

c. Where there is insufficient or out-of-date contact information for an individual affected by a breach, a substitute form of notice may be used:

i. for fewer than 10 individuals, a substitute notice using an alternative form of written notice, telephone, or other means may be provided;

ii. for 10 or more individuals, a substitute notice shall be provided by publishing a conspicuous notice for 90 days on DCS' website home page or in a major print or broadcast media in geographic areas where the individuals affected by the breach likely resides and include a toll-free phone number that remains active for at least 90 days where an individual can learn whether his/her information may be affected by the breach.

d. The written notification shall include, to the extent possible:

i. a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. a description of what types of unsecured protected health information was involved in the breach;

iii. any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. contact procedures for individuals to ask questions and learn additional information.

2. HIPAA Breach Notification for incidents involving DCS employees where the number of affected individuals is 500 or more:

   a. Notification to prominent media outlets serving the state or jurisdiction shall be provided following the discovery of the data breach;

   b. Unless a delay is required by law enforcement, notification shall occur without unreasonable delay and no later than 60 days after discovery of a breach.

3. Non-HIPAA related incidents involving employees or contractors:

   For data incidents involving employees, the Privacy Office will notify individuals affected by the incident.

   If a breach of data is discovered by a contractor, the contractor must notify the Department following the discovery of the breach.

Notification of Department of Health and Human Services

The DCS Privacy Office will notify the U.S. Department of Health and Human Services (DHHS), Office of Civil Rights, no later than 60 days after the end of the year in which a breach of unsecured PHI occurred and must be submitted using the DHHS online submission process or as otherwise prescribed by DHHS. The notice will be sent for breaches involving employees or contractors other than covered entities. A copy of the DHHS notification will be made an attachment to incident's file.

Covered entities contractors are responsible for notifying DHHS, Office of Civil Rights no later than 60 days after the end of the year in which a breach of unsecured protected health information occurred and must be submitted using the DHHS online submission process or as otherwise prescribed by DHHS. A copy of the DHHS notification will be required by the Privacy Office to be attached to incident's file.

VII. FORMS INDEX

HIPAA/PII Privacy Complaint (DCS 1040A)

Notice of Privacy Practices (DCS-1039A)

Property Loss Report (DCS-1117A)

Unusual Incident Report (DCS-1125A)