Information Security **ACCOUNTING OF DISCLOSURES POLICY**	**Issued By (Policy Owner): Chief Information Officer, Information Security Office, and the Privacy Office**
Effective Date: May, 2019	**Last Reviewed: January 2022**

State Administrative Manual (SAM) References		National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) Function and Category	
5310	Privacy	IDENTIFY	Asset Management (ID.AM)
5310.3	Limiting use and disclosure		Governance (ID.GV)
5310.4	Individual access to personal information	PROTECT	Access Control (PR.AC)

1 Accounting of Disclosures Policy

1.1. Introduction and Overview

Disclosure is a release, transfer, access to, or divulging of protected health information (PHI) or Personal Information (PI) outside of California Department of Public Health (CDPH). In general, individuals have the right to know who has received his/her information for reasons other than treatment, payment, or health care operations, or disclosures specifically authorized by the individual.

Examples of this are public health activities (reporting vital statistics, communicable diseases, cancer/tumor registries), reports about victims of abuse, neglect, or domestic violence, releases as a result of a subpoena, disclosures about decedents to coroners, medical examiners, or funeral directors, and other disclosures required by law.

Under HIPAA, disclosures that are not part of treatment, payment, and/or operations and that are not authorized by the patient should be tracked.

Disclosures of personally identifiable information (PII) under the Information Privacy Act (IPA) should also be tracked.

1.2. Objectives

Objectives for this Accounting of Disclosures Policy are to:

1.2.1. Formalize and communicate a consistent approach for maintaining an accounting of disclosures of PHI regarding each individual for at least six years and disclosures of PII regarding each individual for at least three years;

1.2.2. Establish individual's or their personal representative's right to request an accounting of disclosures of the individual's PHI and PII;

1.2.3. Promote accountability to staff for maintaining an accounting of disclosures of PHI and PII; and

1.2.4. Educate staff of their responsibility in maintaining an accounting of disclosures of PHI and PII.

2 Scope and Applicability

This Policy applies to personnel and entities working at, for, or directly on behalf of CDPH.

3 Policy Directives

3.1. **[SHIPM 5.1.1 III. A; SAM 5310.3]:** CDPH shall document, track and maintain information concerning disclosures of health information. This tracking shall document what, when, why and to whom disclosures are made. CDPH shall document, track and maintain information concerning use or disclosures of PII explicitly allowed by Civil Code section 1798.24. This tracking shall document the

date of disclosure, and the name, title, and business address of the individual or state entity to which the disclosure was made.

3.2. **[SHIPM 5.1.1 III. B; SAM 5310.3]:** CDPH shall provide the individual with an accounting of disclosures of their PHI. The accounting shall include disclosures made by CDPH as well as disclosures made to or by Business Associates (BAs) of CDPH.

3.3. An individual or his or her Personal Representative may request an accounting of Accountable Disclosures of the patient's PHI made by CDPH or its Business Associates for up to six years preceding the request. An individual or his or her Personal Representative may request an accounting of Accountable Disclosures of the patient's PII made by CDPH for up to three years preceding the request. The individual may make the request for an accounting in writing or orally. If the request is made orally, CDPH shall document such request. CDPH shall retain this request and a copy of the written accounting that was provided to the individual, as well as the name/departments responsible for the completion of the accounting.

3.4. The request for an accounting of disclosure of PHI or PII shall be submitted to CDPH's Privacy Officer at the following address or phone number:

Privacy Office Email Address: **Privacy@CDPH.ca.gov**

Privacy Office Phone Number: **(916) 440-7671**

3.5. An individual may authorize in writing that the accounting of disclosures be released to another individual or entity. The request shall clearly identify information required to carry out the request (name, address, phone number, etc.).

3.6. **[SHIPM 5.1.1 III. B. 1]: Timing of response to an accounting of disclosure request**: CDPH shall respond to a request for an accounting of disclosures no later than 60 days after receipt of such a request. If unable to respond within this period of time, CDPH may extend the time by no more than 30 days provided that, within the initial 60-day period, CDPH provides the individual with a written statement of the reasons for the delay and the date by which the accounting will be provided. Only one (1) 30-day extension is permitted.

3.7. **[SHIPM 5.1.1 III. B. 2. (a)-(d); NIST 800-53 AR-8]: Content of disclosures accounting:** The accounting for each disclosure of PHI shall include the following, at a minimum:

3.7.1. The date(s) of the disclosure(s);

3.7.2. The name and title of the entity or person to whom the information was provided, and their recorded address;

3.7.3. A brief description of the health information disclosed;

3.7.4. A brief statement describing the reason for the required or permitted disclosure (e.g., pursuant to a subpoena), or a copy of the written request if applicable.

Special Note: Subsequent individual requests for accounting of disclosures, within 12 months of the first accounting of disclosure, need only include incremental disclosures made since the original accounting

3.8. <u>Approval of disclosures accounting.</u>

3.8.1. If no temporary suspension of the right to an accounting of disclosures is in effect, and no other reason for denying the request has been identified, the CDPH Privacy Officer and designated program officials shall compile an accounting of disclosures of the records that will include the following:

3.8.1.1. Manners of release of the PHI and PII (hard copy, verbal, and electronic)

3.8.1.2. The disclosures of PHI to Business Associates, and

3.8.1.3. Disclosures of PHI by Business Associates

3.8.2. CDPH shall provide the accounting of disclosures to the requesting individual or his/her personal representative within sixty (60) days of the date of the request, and

3.8.3. If CDPH is not able to provide the accounting of disclosures within 60 days of the date of the request, the CDPH Privacy Officer or designated program officials may extend the time to provide the accounting by no more than 30 days, provided that:

3.8.3.1. CDPH gives the individual or his/her personal representative, within the initial 60 days, a written statement of the reasons for the delay and the date by which the accounting will be provided, and

3.8.3.2. CDPH may use no more than one extension of time for action on a request for an accounting.

3.9. **[SHIPM 5.1.1 III. B. 3. (a)-(b)]: Charge for the accounting:**

3.9.1. The first accounting of disclosures made to an individual during 12-month period shall be provided free of charge.

3.9.2. For subsequent request for an accounting of disclosures made by the same individual within this 12-month period, CDPH may impose a reasonable, cost-based fee for the accounting, provided that the individual is informed in advance of the fees that will be charged and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting to avoid or reduce the fee.

3.10. **[SHIPM 5.1.1 III. C. (1)-(6)]: Exceptions to required disclosure accounting:** The following types of disclosures are excluded from the accounting of PHI disclosures requirement:

3.10.1. Disclosures made for treatment, payment, and health care operations;

3.10.2. Disclosures made to the individual about themselves;

3.10.3. Disclosures resulting from or incident to otherwise permitted disclosure;

3.10.4. Disclosures made pursuant to an authorization;

3.10.5. Disclosures made for a facility's directory, or to persons involved in the patient's care or for related purposes; and

3.10.6. Disclosures that are part of a limited data set.

3.11. **[SHIPM 5.1.1 III. D. (1)-(7)]: PHI disclosure accounting for research purposes:** If during the period of time covered by the requested accounting, CDPH makes disclosures of PHI for specific research purposes regarding 50 or more individuals' records, CDPH may account for the disclosures by providing the following:

3.11.1. The name of the protocol or other research activity;

3.11.2. A plain language description of the research protocol or activity, including the purpose of the research and the criteria for selecting certain records;

3.11.3. A brief description of the type of health information that was disclosed;

3.11.4. The dates or periods of time during which the disclosures occurred, or may have occurred, including the date of the last disclosure during the accounting period;

3.11.5. The name, address, and telephone number of the entity that sponsored the research and the researcher to whom the information was disclosed;

3.11.6. A statement that the health information may or may not have been disclosed for a particular protocol or particular research activity; and

3.11.7. If it is reasonably likely that the health information was disclosed for a research protocol or activity, CDPH shall, if requested by the individual, assist the individual in contacting the entity that sponsored the research and the researcher.

3.12. Suspension of the Right to an Accounting.

3.12.1. **[45 C.F.R. § 164.528(a)(2)(i)]: Written Requests for Suspensions:** CDPH shall temporarily suspend an Individual's right to a PHI accounting in accordance with the HIPAA Privacy Rule for a specified time if requested by a Health Oversight Agency or Law Enforcement Official in writing. If requested to suspend accounting, CDPH should request each Health Oversight Agency or Law Enforcement Official to state, in writing, that the accounting could be reasonably likely to impede the Agency's activities and the time period for the required suspension prior to implementing the suspension.

3.12.2. **[45 C.F.R. § 164.528(a)(2)(ii)]: Oral Requests for Suspensions*:*** CDPH shall also abide by the oral request(s) of a Health Oversight Agency or Law Enforcement Official for the temporary suspension of an individual's right to a PHI accounting. CDPH shall also document the name of the agency or official and the statement requesting the suspension and will limit the suspension to no longer than 30 days unless a written statement from the agency/official is received.

3.13. **[SHIPM 5.1.1 III. E; SAM 5310.3; NIST 800-53 AR-8]: Documentation:** CDPH is responsible to retain disclosure documentation related to PHI for a period of six (6) years from the date of its creation, or the date when it last was in effect, whichever is greater. CDPH is responsible to retain disclosure documentation related to PII for a period of three (3) years from the date of its creation, or the date when it last was in effect, whichever is greater. Disclosure documentation related to public, confidential or sensitive information shall be retained per the appropriate record retention schedule.

3.14. **[SHIPM 5.1.1 III. E]:** CDPH's Business Associate Agreements (BAA) shall include a requirement that Business Associates document, track and account for disclosures required to comply with an accounting of disclosures. In addition, the BAA shall address how and when (timeframe) the Business Associate is to provide CDPH with the information required to comply with an accounting when requested by the individual.

4 Roles and Responsibilities

CDPH Policy Owner

4.1. CDPH Policy Owner is responsible for determining the appropriate audience(s) for this policy.

4.2. CDPH Policy Owner shall create awareness about the policy and educate the identified audience(s) of their individual responsibilities and the associated sanctions.

4.3. CDPH Policy Owner is responsible for the periodic review and update of the policy.

4.4. CDPH Policy Owner is responsible for supporting the periodic auditing and assessment of compliance with the policy.

4.5. CDPH Policy Owner is responsible for seeking guidance from Information Security Officer (ISO), Chief Information Officer (CIO), Privacy Officer and Subject Matter Experts (SMEs) as appropriate to comply with security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs.

4.6. CDPH Policy Owner is responsible for supporting and coordinating the standards, procedures and guideline development activities required aligning with the overarching policy.

4.7. CDPH Policy Owner is responsible for including the approved policy into the policy management system and the completeness of relevant metadata fields.

4.8. CDPH Policy Owner is responsible for responding to workflow notifications that may require review, impact analysis, policy changes and policy approval.

4.9. CDPH Policy Owner is responsible for managing the policy throughout its lifecycle from development to decommissioning or archiving.

4.10. CDPH Policy Owner is responsible for communicating key notifications regarding the policy such as decommissioning to linked policies, procedures, standards and guidelines to relevant stakeholders.

4.11. CDPH Policy Owner is responsible for participating in the security and privacy variance process and assessing the risks and compliance plan associated with variance requests.

4.12. CDPH Policy Owner supports the development of processes and metrics required to measure the effectiveness of the policy.

CDPH Privacy Officer

4.13. CDPH Privacy Officer is responsible to include the requirements for accounting of disclosures in the contracts being signed with contractors / sub-contractors.

4.14. CDPH Privacy Officer is responsible for confirming individuals or their Personal representative's right to request an accounting of accountable disclosures of the individual's PHI or PII.

4.15. CDPH Privacy Officer is responsible to temporarily suspend an individual's accounting right in accordance with the privacy regulations for a specified time if requested by a Health oversight agency or law enforcement official in writing.

4.16. CDPH Privacy Officer is overseeing the CDPH's implementation of accounting of disclosure policy and compliance with State and Federal privacy laws, including the California Information Practices Act (IPA) and the Federal Health Insurance Portability and Accounting Act (HIPAA) privacy regulations.

CDPH System Owners, Data Custodians and/or Program Management

4.17. Systems Owners and Data Custodians should assist the privacy office in maintaining accounts of disclosures as required by State and Federal privacy laws, including the California Information Practices Act (IPA) and the Federal Health Insurance Portability and Accounting Act (HIPAA) privacy regulations.

4.18. System Owners and Data Custodians should assist the privacy office in receiving and responding to patient's request for accounting of disclosures.

4.19. Systems Owners and Data Custodians are responsible to check with privacy officers of suspension request before fulfilling request for accounting of disclosure.

CDPH Users

4.20. CDPH Users are responsible for familiarizing themselves with accounting of disclosure policies and associated procedures.

4.21. CDPH Users are responsible for reporting incidents of possible misuse or violation of this policy to the CDPH Privacy Officer, Information Security Officer (ISO), designee or appropriate security / privacy staff.

4.22. CDPH personnel are required to read and understand this policy and applicable CDPH information security and privacy policies.

Table 1 RACI Matrix

Activity	CIO	CISO	Privacy Team	Policy Owner	CDPH Users
Own Policy	C	C	R	A	-
Policy awareness	R	R	R	A	I
Develop and maintain supporting guidelines, standards, procedures and processes	C, I	C, I	R	A	I
Report violations	R	R	R	R	R
Review /Approve Security Variances	C, I	I	C	A	-

R	Responsible
A	Accountable
C	Consult
I	Inform

5 Enforcement

5.1 Non-compliance with this policy may result in disciplinary action in compliance with the escalating CDPH disciplinary process up to, and including, termination.

The consequences of CDPH negligence and non-compliance with state laws and policies may include loss of delegated authorities, negative audit findings, monetary penalties and legal actions.

As set forth in Government Code section 11549.3, CDPH shall comply with the information security and privacy policies, standards, procedures, and guidelines issued by the California Office of Information Security. In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the *[OIS]*, CDPH shall comply with security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, Information Security Officer (ISO), and Privacy Program Officer/Coordinator to identify security and privacy requirements applicable to their programs and implementation of the requisite controls.

6 Auditing

6.1 CDPH has the right to audit activities related to the use of State information assets.

7 Reporting

7.1 Violations of this policy should be reported to the CDPH information security officer and privacy officer.

8 Security Variance Process

8.1. If compliance is not feasible or is technically impossible, or if deviation from this policy is required to support a business function, the respective manager should formally request a security variance as defined in the CDPH Security Variance process.

9 Authoritative Sources

9.1 NIST Special Publication (SP) 800-53 Reference

Family	Control
Accountability, audit, and risk management	AR-8 Accounting of disclosures
Individual participation and redress	IP-2 Individual access

9.2 Statewide Health Information Policy Manual (SHIPM) Reference

Reference	Control
Accounting of Disclosures	SHIPM 5.1.0
Uses and Disclosures	SHIPM 2.2.0
Patient Rights – Access	SHIPM 5.4.0

9.3 Statewide Administrative Manual (SAM) References and Implementation Guidance

Reference	Article
5310.3	5310.3 Limiting Use and Disclosure

9.4 Statewide Information Management Manual (SIMM) References and Implementation Guidance

Reference	Article
5300-B	5300-B Foundational Framework

10 Related Policies, Procedures and Standards

Reference	Article
Information Security Policies	140 Roles & Responsibilities

Reference	Article
Information Security Policies	180 Regulation & Enforcement
Information Security Policies	190 Variance Process
Statewide Health Information Policy Manual (SHIPM)	Section: 5.1.0 – Accounting of Disclosures
Statewide Health Information Policy Manual (SHIPM)	Section: 2.2.0 – Uses and Disclosures
Statewide Health Information Policy Manual (SHIPM)	Section: 5.4.0 – Patient Rights - Access
Statewide Administrative Manual (SAM)	Section 5310.3 – Limiting Use and Disclosure

11 Revision History

Date	Revision	Description of Change
March, 2018	1.0	Initial Version

12 Definitions of Key Terms

CDPH uses the information security and privacy definitions issued by the California Department of Technology Office of Information Security in implementing information security and privacy policy. Terms and definitions are defined here and are on the California Department of Technology website at https://cdt.ca.gov/security/technical-definitions/.

Information Assets	Information Assets include (a) categories of paper and automated information, including (but not limited to) records, files, and databases; and (b) information technology facilities and equipment (including telecommunications networks, personal computer systems, laptops, tablets and mobile devices), and software owned or leased by state entities.
Information Asset Custodian	Personnel or organizational unit (such as a data center or information processing facility) responsible as caretaker for the proper use and protection of information assets on behalf of the information asset owner.
NIST	NIST stands for the National Institute of Standards and Technology https://www.nist.gov/

Owner of Information Assets	An organizational unit having responsibility for making classification, categorization and control decisions regarding information assets.
Personally Identifiable Information (PII)	Personally Identifiable Information (PII) means any information that is maintained by CDPH that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.
Protected Health Information (PHI)	"Protected Health Information" is defined as Individually Identifiable Health Information that is transmitted electronically, maintained electronically or transmitted or maintained in other form or medium, concerning CDPH patient or the patient of healthcare provider of CDPH.

13 Policy Approval

Position	Name	Signature	Date
Privacy Officer	Ryan Davis		