County of Sacramento

Health Insurance Portability and Accountability Act

HIPAA Privacy Rule Policies and Procedures

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

HIPAA PRIVACY OFFICER & SECURITY OFFICER: Rami Zakaria

Office of Compliance
799 G Street, Suite 217
Sacramento, CA 95814
(916) 874-2999
HIPAAOffice@saccounty.gov

Intranet: www.inside.compliance.saccounty.gov
Internet: www.compliance.saccounty.gov

County of Sacramento HIPAA Privacy Rule Policies and Procedures

TABLE OF CONTENTS

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

The HIPAA Privacy Rule Policies and Procedures, and all forms referred to in the Policies and Procedures, may be accessed electronically at http://inside.compliance.saccounty.net.

County of Sacramento HIPAA Privacy Rule Policies and Procedures
DEFINITIONS

Terms	Definitions
Access	The ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.[1]
Administrative Safeguards	Administrative actions and policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the County's or business associate's workforce in relation to the protection of that information.[2]
Authorization	Consent of the client, whether written or oral.[3]
Breach	The acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule. A breach does not include: 1) Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity if made in good faith and within the scope of the authority, with no further use or disclosure; 2) Any inadvertent disclosure by a person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, to any authorized person, and the PHI is not further used or disclosed; 3) Any disclosure of PHI where the covered entity or business associate has a good faith belief the unauthorized person would not reasonably have been able to retain such information. The covered entity or business associate must be able to demonstrate that there is a low probability that the information has been compromised based on a risk assessment of at least the following: 1) The nature and extent of the PHI involved, including the

[1] 45 CFR 164.304 "Definitions"
[2] 45 CFR 164.304 "Definitions
[3] 45 CFR 164.508 "Uses and disclosures for which an authorization is required"

Terms	Definitions
	identifiers; 2) The unauthorized person who used the PHI or to whom the disclosure was made; 3) Whether the PHI was actually acquired or viewed; and 4) The extent to which the risk to the PHI has been mitigated.[4]
Business Associate	A person or organization (or their subcontractor), who is not a member of the covered entity's workforce, who creates, receives, maintains, or transmits protected health information (PHI) or electronic protected health information (EPHI) on behalf of a HIPAA covered component. Services that a Business Associate (BA) provide include: claims processing or administration; data analysis, processing and/or administration; utilization review; quality assurance; billing; benefit management; document destruction; temporary administrative support; legal; actuarial; accounting; consulting; information technology (IT) support; health information organizations; e-prescribing gateways or providers of data transmission services; and certain patient safety activities. A covered entity may be a Business Associate of another covered entity, but is not a health care provider with respect to disclosures by the covered entity concerning treatment of the individual.[5]
Client	An individual who is receiving HIPAA covered health services from the County of Sacramento or enrolled in a County health plan.
Contrary	When used to compare a provision of State law to a standard, requirement or implementation specification, means: A covered entity or business associate would find it impossible to comply with both the State and federal requirements; or The provision of State law stands as an obstacle to carrying out the full purposes and objectives of the federal requirements.[6]
Confidentiality	Ensuring that data or information is not made available or disclosed to unauthorized persons or processes.[7]

[4] 45 CFR 164.402 "Definitions"
[5] 45 CFR 160.103 "Definitions"
[6] 45 CFR 160.202 "Definitions"
[7] 45 CFR 164.304 "Definitions"

Terms	Definitions
Correctional Institution	Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house or residential community program center operated by, or under contract to the federal, state, or local government for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Includes juvenile offenders adjudicated delinquent by the court, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.[8]
Covered component	See: health care component.
Covered entity	A health plan, health care clearinghouse or health care provider who transmits any health information in electronic form in connection with a transaction to carry out financial or administrative activities related to health care. (A covered entity may also maintain protected health information in paper records.)[9]
DHHS	Unless otherwise specified, DHHS will always refer to the United States (U.S.) Department of Health and Human Services.[10]
De-Identified Health Information	Information that does not identify an individual because identifiers have been removed. Identifiers include name; address; geographic subdivisions smaller than a state; dates; phone and fax numbers; email addresses; URLs; IP addresses; biometric identifiers; medical record, social security, health plan beneficiary, certificate/license and account numbers; vehicle identification numbers; photographic images; and any other unique identifier.[11]
Designated record set	A group of records maintained by or for a covered entity that: a) Are the medical records and billing records about individuals maintained for or by a covered health care provider; b) Are the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or c) Are used, in whole or in part by or for the covered entity to make decisions about individuals. For purposes of this definition, the term record means any item,

[8] 45 CFR 164.401 “Definitions”
[9] 45 CFR 160.103 “Definitions”
[10] 45 CFR 160.103 “Definitions”
[11] 45 CFR 164.514 “Other requirements relating to uses and disclosures of protected health information”

Terms	Definitions
	collection or grouping of information that includes PHI and is maintained, used, collected or disseminated by or for a covered entity.[12]
Disclosure	The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.[13]
EHR	Electronic Health Record (also known as an EMR – Electronic Medical Record) means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.[14]
Electronic media	1.) Electronic storage material on which data is or may be recorded electronically, including devices in computers (hard drives) or any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. 2.) Transmission media used to exchange data already in electronic storage media, such as the internet (wide-open), extranet or intranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and physical movement of removable/transportable electronic storage media.[15]
Encryption	Scrambling or encoding electronic data to prevent unauthorized access or use. Only individuals with knowledge of a password or key can decrypt (unscramble) the data. Encryption methods use an algorithmic process that transforms the data into a form in which there is a low probability of assigning meaning to it without the use of a confidential process or key.[16]
ePHI	Protected health information (PHI) that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. *See also Protected Health Information.*
E-prescribing Gateway	An organization, usually commercial, providing an electronic network connection for the purpose of transmitting medical prescriptions from a HIPAA covered health care provider to an external pharmacy through standardized electronic messages that both the prescriber's

[12] 45 CFR 164.501 "Definitions
[13] 45 CFR 160.103 "Definitions"
[14] 42 CFR USC 17921 Section 13400 "Definitions"
[15] 45 CFR 160.103 "Definitions"
[16] 45 CFR 164.304 "Definitions"

Terms	Definitions
	system and the pharmacist's system must implement. An e-prescribing Gateway organization is required to be a Business Associate of the covered entity.[17]
Genetic Information	Protected Health Information (PHI). Any individual's genetic tests*, or those of family members* of the individual; the manifestation of a disease or disorder in family members of such individual, any request for, or receipt of, genetic services or clinical research including genetic services. Genetic information excludes information about the sex or age of the individual.[18]
Group Health Plan	An individual or group plan that provides, or pays the cost of, medical care.[19]
Health care component	A component or combination of components of a hybrid covered entity designated by the entity in accordance with 45 CFR §164.105(a)(2)(iii)(D) that perform HIPAA covered functions or activities that would make such a component a Business Associate contractor of a component that performs covered functions if the two components were separate legal entities.[20]
Health care operations	The following are examples of activities of the covered entity meeting the definition of health care operations: 1) Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management, care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; 2) Competence or qualifications review of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs for health care providers with supervision, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; 3) Underwriting, premium rating and other activities relating to creation, renewal or replacement of a health insurance contract or

[17] No federal regulation definition was found. The Omnibus Final Rule Executive Summary states that e-prescribing Gateway was "included as merely illustrative of the types of organizations that would fall within…the definition of "business associate."
[18] 45 CFR 164.103 "Definitions"
[19] Public Health Service Act, 42 USC 300gg-91(a)(2)
[20] 45 CFR 164.103 "Definitions"

Terms	Definitions
	health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable; 4) Medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; 5) Business planning and development, such as cost-management and planning-related analyses related to managing and operating the entity; 6) Business management and general administrative activities of the entity, including, but not limited to: customer service, resolution of internal grievances, the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity.[21]
Health Information Organization (HIO)	Performs activities on behalf of one or more HIPAA covered entities to manage the exchange of PHI through an electronic network. In that role, HIOs are defined by HIPAA as Business Associates of the covered health care providers. Also known as a Health Information Exchanges (HIEs), they may be governmental, non-profit or for profit organizations.[22]
HIPAA – 45 CFR	The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996 to ensure that individuals' health information is protected while allowing the flow of health information required to provide high quality health care. It is referred to as 45 CFR (Congressional Federal Register). *Part 160* deals with General Administrative Requirements; *Part 164* concerns Security and Privacy. The main sections of Part 164 are: Subpart C: known as the **Security Rule** (protection of electronic protected health information - EPHI); Subpart D: known as the **Notification Rule** in case of a breach of unsecured protected health information; and Subpart E: known as the **Privacy Rule** (standards to ensure the privacy of individually identifiable health information.)
HITECH Act	Health Information Technology for Economic and Clinical Health (HITECH) Act is Title XIII of Division A of the American Recovery and Reinvestment Act of 2009 (ARRA) signed on February 17, 2009. HITECH contains privacy and security enhancements to HIPAA,

[21] 45 CFR 164.501 "Definitions"

[22] No federal regulation definition was found. The Omnibus Final Rule Executive Summary states that Health Information Organization (HIO) was "included as merely illustrative of the types of organizations that would fall within…the definition of "business associate."

Terms	Definitions
	financial incentives, grants and loans for adopting electronic health records (EHRs) and increased penalties for HIPAA violations.[23]
Hybrid entity	A single legal entity that is covered by HIPAA, whose business activities include both covered and non-covered functions.[24]
Institutional Review Board (IRB)	A committee formally designated by a covered entity to approve, monitor, and review medical research with the aim to protect the rights and welfare of the research subjects. IRBs are regulated by the U.S. DHHS. [25]
Individually Identifiable	Information that is a subset of health information, including demographic information collected from an individual, and either directly identifies that individual or it is reasonable to expect that the information can identify the individual. (See also Protected Health Information.)[26]
Inmate	A person incarcerated in or otherwise confined to a correctional institution.[27]
Law Enforcement Official	An officer or employee of any agency or authority of the United States, a State, territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.[28]
Lawful Custody	The detainer of an individual by virtue of a lawful authority. To be in custody is to be lawfully detained under arrest.[29]
Limited Data Set	A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii)

[23] Public Law 111-5
[24] 45 CFR 164.103 “Definitions”
[25] 45 CFR 46.102 “Definitions”
[26] 45 CFR 160.103 “Definitions”
[27] 45 CFR 164.501 “Definitions”
[28] 45 CFR 164.103 “Definitions”
[29] 45 CFR 164.501 “Definitions”

Terms	Definitions
	Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.[30]
Minimum Necessary	Use and disclosure of protected health information (PHI), other than for treatment, payment or health care operations, is limited to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. The covered entity or business associate disclosing PHI is the one who determines the "minimum necessary".[31]
Omnibus Rule	Modifications to the HIPAA, Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act (GINA); and other modifications to the HIPAA Rules. Effective date: March 26, 2013; compliance date: September 23, 2013.[32]
Payment	Payment means the activities undertaken by: 1. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or 2. A health care provider or health plan to obtain or provide reimbursement for the provision of health care. Payment activities include, but are not limited to: a) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; b) Risk adjusting amounts due based on enrollee health status and demographic characteristics; c) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; d) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

[30] 45 CFR 164.514(e)(2) "Implementation specification: Limited data set"
[31] 45 CFR 164.502 (b) "Standard: Minimum Necessary" and 164.514 (d) "Standard: Minimum necessary requirements"
[32] Federal Register / Vol. 78, No. 17 / January 25, 2013 / Rules and Regulations

Terms	Definitions
	e) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and f) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address, date of birth, social security number, payment history, account number, and name and address of the health care provider and/or health plan. [33]
Physical safeguards	Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.[34]
Plan Administration Functions	Administrative functions performed by a group health plan sponsor on behalf of the group health plan, excluding functions performed by the plan sponsor in connection with any other benefit or benefit plan of the sponsor.[35]
Protected Health Information (PHI)	PHI is health information that a covered entity creates or receives, that identifies an individual, and relates to: • The individual's past, present, or future physical or mental health or condition; • The provision of health care to the individual; or • The past, present, or future payment for the provision of health care to the individual. PHI includes written, spoken and electronic forms. PHI is "individually identifiable information". PHI excludes individually identifiable information in education records, school health records covered by FERPA (Family Educational Rights and Privacy Act), employment records held by a covered entity in its role as employer, or records regarding a person who has been deceased for more than 50 years.[36]
Public Health Authority	An agency or authority of the federal government, state, territory or political subdivision of a state or territory, or a person or entity acting under grant of authority from such public agency, including the

[33] 45 CFR 164.501 "Definitions"
[34] 45 CFR 164.304 "Definitions
[35] 45 CFR 164.504 "Definitions"
[36] 45 CFR 160.103 "Definitions"

Terms	Definitions
	employees or agents of the public agency, that is responsible for public health matters as part of its official mandate.[37]
Reasonable Cause	An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision [under HIPAA], but in which the covered entity or business associate did not act with willful neglect.[38]
Required by Law	A mandate contained in law that compels a HIPAA covered entity to make a use or disclosure of protected health information (PHI) and that is enforceable in a court of law.[39]
Research	A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.[40]
Risk Assessment	A process of assessing those factors that could affect confidentiality, availability, and integrity of key information assets and systems. HIPAA covered components are responsible for ensuring the integrity, confidentiality, and availability of PHI, electronic PHI and equipment that contains it, while minimizing the impact of security procedures and policies upon business productivity.
Security or Security Measures	All of the administrative, physical and technical safeguards in an information system.[41]
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification of destruction of protected health information, or interference with system operations in an information system containing protected health information.[42]
Summary Health Information	Information that may be individually identifiable health information that summarizes the claims history, claims expenses, or types of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan, and which meets the standards for de-identification of PHI described in Privacy Rule

[37] 45 CFR 164.501 “Definitions”
[38] 45 CFR 160.401 “Definitions”
[39] 45 CFR 164.103 “Definitions”
[40] 45 CFR 164.501 “Definitions”
[41] 45 CFR 164.304 “Definitions”
[42] 45 CFR 164.304 “Definitions”

Terms	Definitions
	Policy AS-100-07: "De-identification of Protected Health Information and Use of Limited Data Sets".[43]
Technical Safeguards	The technology and policy and procedures that protect and control access to electronic protected health information (ePHI).[44]
Treatment	The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.[45]
Unsecured PHI	Protected health information (PHI) that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through use of a technology or methodology such as encryption, or otherwise specified by the Secretary of DHHS in the guidance issued under section 13402(h)(2) of Public Law 111-5.[46]
Valid ID (Identification)	Required forms of identification for release of PHI, established either by HIPAA (in the case of a public official or person acting on behalf of a public official) or by County policy to verify identity and authority of a person requesting access, restriction, amendment or disclosure of PHI.[47]
Workforce / Workforce Member	Employees (including supervisors, managers and line staff), volunteers, trainees, and other persons whose conduct, in the performance of work for a HIPAA covered entity or Business Associate, is under the direct control of such entity or business associate, whether or not they are paid by the covered entity or Business Associate.[48]
Workstation	An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions and any electronic media stored in its immediate environment.[49]

[43] 45 CFR 164.504 "Definitions"
[44] 45 CFR 164.304 "Definitions"
[45] 45 CFR 164.501 "Definitions"
[46] 45 CFR 164.402 "Definitions"
[47] 45 CFR 164.514 (h)(1) "Standard: Verification requirements"
[48] 45 CFR 160.103 "Definitions"
[49] 45 CFR 164.304 "Definitions

Policy AS-100-01: General Privacy

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow, please contact the Office of Compliance or County Counsel.

Purpose:

The intent of this policy is to outline the manner in which the County of Sacramento meets the requirements of 45 Code of Federal Regulations (CFR), Part 164, known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These policies provide general guidelines and expectations for the necessary collection, use, and disclosure of protected health information (PHI) about individuals in order to provide services and benefits to individuals, while maintaining reasonable safeguards to protect the privacy of their PHI. These policies are applicable to all units, divisions, programs or departments within the County of Sacramento which are designated HIPAA-covered components of the County's hybrid entity.

For the purpose of these policies, the terms "confidential information", "health confidential information", individual health confidential information", "protected health confidential information", "protected health information", "PHI", "electronic protected health information", and "ePHI" are the same. These terms mean information that:

a. Is a subset of health confidential information, including demographic confidential information collected from an individual, and

b. Is created, received, maintained, or transmitted by a health care provider, health plan, health care clearinghouse, or business associate; and

c. Relates to the:

    i. Past, present, or future physical or mental health or condition of an individual; or,

ii. The provision of health care to an individual; or,

iii. The past, present, or future payment for the provision of health care to an individual; and

d. Either:

i. Identifies the individual; or,

ii. The confidential information creates a reasonable basis to believe it can be used to identify the person; and,

e. Is:

i. Transmitted by electronic media; or

ii. Maintained in electronic media; or

iii. Transmitted or maintained in any other form or medium, and

f. Does not include:

i. Employment records; or,

ii. Education records

iii. Records under the Family Educational and Right to Privacy Act (FERPA).

Policy:

1. General

County of Sacramento will safeguard PHI about Individuals.

a. The County of Sacramento may collect, maintain, use, transmit, share and/or disclose confidential information about individuals to the extent needed to administer the County of Sacramento programs, services and activities. Confidential Information collected will be safeguarded in accordance with policy.

b. The County of Sacramento will safeguard all confidential information about individuals, inform individuals about the County of Sacramento's privacy practices and respect individual privacy rights, in accordance with policy.

c. This policy identifies four types of individuals on whom County of Sacramento is most likely to obtain, collect, maintain or transmit information:

i. County of Sacramento Clients;

ii. Providers

iii. County of Sacramento Inmates;

iv. County of Sacramento employees enrolled in health benefits.

d. The County of Sacramento shall provide training to all workforce members in programs constituting a "covered entity" or a "health care component" in designated HIPAA-covered components of the County's hybrid entity as those terms are defined by HIPAA in the County of Sacramento' privacy policies, and shall require every workforce member to sign a County of Sacramento Form 3013, "HIPAA Privacy & Security Policy & Procedures Acknowledgement Form**"** or complete an electronic HIPAA Training acknowledgement outlining their role and responsibilities relating to protecting the privacy of County of Sacramento clients.

2. Safeguarding confidential information about Clients

A "Client" is an individual who requests or receives health services from County of Sacramento.

a. The County of Sacramento, its workforce members, and business associates shall respect and protect the privacy of records and PHI about clients who request or receive services from County of Sacramento. This includes, but is not limited to:

i. Applicants or enrollees in a County operated health plan;

ii. Minors and adults receiving alcohol and drug, mental health, primary health and public health services from County of Sacramento;

iii. Persons who apply for or are admitted to a county operated or county funded mental health center;

b. All PHI on County of Sacramento clients must be safeguarded in accordance with County of Sacramento privacy policies and procedures.

c. The County of Sacramento shall not use or disclose PHI unless either:

i. The client has authorized the use or disclosure in accordance with County of Sacramento Policy AS-100-03, "Use and Disclosures of Client Protected Health Information;" or

ii. The use or disclosure is specifically permitted under County of Sacramento

Policy AS-100-03, “Use and Disclosures of Client Protected Health Information.”

d. County of Sacramento program offices shall adopt procedures to reasonably safeguard client PHI.

3. Safeguarding confidential information about Health Plan Enrollees

A health plan enrollee (“Enrollee”) is any Covered Person enrolled in one or more of the group health plans sponsored by the County of Sacramento, which results in the County of Sacramento having possession of or access to protected health information.

a. When County of Sacramento obtains PHI about Enrollees, County of Sacramento may use and disclose such PHI consistent with federal and state law and regulation.

4. Conflict with other requirements regarding privacy and safeguarding

a. County of Sacramento has adopted reasonable policies and procedures for administration of its programs, services and activities. If any state or federal law or regulation, or order of a court having appropriate jurisdiction, imposes a stricter requirement upon any County of Sacramento policy regarding the privacy or safeguarding of protected health information, County of Sacramento shall act in accordance with that stricter standard.

b. In the event that more than one policy applies but compliance with all such policies cannot reasonably be achieved the County of Sacramento workforce member will seek guidance according to established County of Sacramento policy and procedures. County of Sacramento workforce should first consult with their Program Manager, the County of Sacramento Office of Compliance, or County Counsel in appropriate circumstances.

5. County of Sacramento Notice of Privacy Practices

a. County of Sacramento will make available a copy of the County of Sacramento 2090, “County of Sacramento Notice of Privacy Practices,” to any client covered by HIPAA applying for or receiving covered services from the County of Sacramento or enrolled in a County health plan.

b. The County of Sacramento Notice of Privacy Practices shall contain all information required under federal regulations regarding the notice of privacy practices for PHI under HIPAA.

c. Where County of Sacramento is a healthcare provider, County of Sacramento will seek to acquire a signed acknowledgement, County of Sacramento Form

2092, “Notice of Privacy Practices, Acknowledgement of Receipt,” or the Division of Behavioral Health Services Acknowledgement of Receipt, from each client at the first service delivery or as soon as practicable.

d. Inmates do not have a right to Notice of Privacy Policies.

6. Client Privacy Rights

The County of Sacramento policies and procedures, as well as other federal and state laws and regulations, outline the HIPAA covered client’s right to access their own protected health information, with some exception. These policies also describe specific actions that a client can take to request restrictions or amendments to their protected health information, and the method for filing complaints. These specific actions are outlined in County of Sacramento HIPAA Privacy Rule Policy AS-100-02, “Client Privacy Rights.”

7. Use and Disclosures of PHI

County of Sacramento shall not use or disclose any PHI about a HIPAA covered client of County of Sacramento programs or services without a signed authorization for release of that PHI from the individual, or the individual’s personal representative, *unless* authorized by this policy, or as otherwise allowed or required by state or federal law, as outlined in County of Sacramento Privacy Rule Policy AS-100-03, “Use~~s~~ and Disclosure~~s~~ of Client Protected Health Information.”

8. Minimum Necessary Standard

a. County of Sacramento will use or disclose only the minimum amount of PHI necessary to provide services and benefits to HIPAA covered clients, and only to the extent provided in County of Sacramento policies and procedures.

b. This standard does not apply to:

i. Disclosures to or requests by a health care provider for treatment;

ii. Uses or disclosures made to the individual;

iii. Uses or disclosures authorized by the individual;

iv. Disclosures made to the Secretary of the United States Department of Health and Human Services in accordance with federal HIPAA regulations at 45 CFR 160, Subpart C.

v. Uses or disclosures that are required by law; and

vi. Uses or disclosures that are required for compliance with federal HIPAA

regulations at 45 CFR, Parts 160 and 164.

c. When using or disclosing an individual's PHI, or when requesting an individual's PHI from a provider or health plan, County of Sacramento employees must make reasonable efforts to limit the amount of PHI to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request, as outlined in County of Sacramento Policy AS-100-04, "Minimum Necessary Standard."

9. Administrative, Technical and Physical Safeguards

County of Sacramento staff must take reasonable steps to safeguard PHI from any intentional or unintentional use or disclosure, as outlined in County of Sacramento Policy AS-100-05, "Administrative, Technical, and Physical Safeguards."

10. Use and Disclosures for Research Purposes and Waivers

The County of Sacramento may use or disclose an individual's PHI for research purposes as outlined in County of Sacramento Privacy Rule Policy AS-100-06, "Uses and Disclosures for Research Purposes and Waivers." This policy specifies requirements for using or disclosing PHI with and without an individual's authorization, and identifies some allowable uses and disclosure of PHI when County of Sacramento is acting as a Public Health Authority.

11. De-Identification of PHI and Use of Limited Data Sets

The County of Sacramento staff will follow standards under which client PHI can be used and disclosed if information that can identify a person has been removed (de-identified) or restricted to a limited data set. Unless otherwise restricted or prohibited by other federal or state law, County of Sacramento can use and share information as appropriate for the work of County of Sacramento, without further restriction, if County of Sacramento or another entity has taken steps to de-identify the PHI as outlined in County of Sacramento HIPAA Privacy Rule Policy AS-100-07, "De-identification of Protected Health Information and Use of Limited Data Sets."

12. Business Associate Relationships

County of Sacramento may disclose PHI to business associates with whom there is a written contract or memorandum of understanding as outlined in County of Sacramento HIPAA Privacy Rule Policy AS-100-08, "Business Associates." Business Associates and their subcontractors have responsibilities under HIPAA to protect and safeguard client's confidential information.

13. Enforcement, Sanctions and Penalties for Violations of Individual Privacy

All workforce members, including employees, contract employees, volunteers, interns and members of the County of Sacramento workforce must guard against improper uses or disclosures of County of Sacramento client information. County of

Sacramento shall apply appropriate sanctions against members of its workforce as outlined in County of Sacramento Policy AS-100-09, “Enforcement, Sanctions, and Penalties.”

Form(s):

- County of Sacramento HIPAA Form 2090, “County of Sacramento Notice of Privacy Practices”
- County of Sacramento HIPAA Form 2092, “County of Sacramento Notice of Privacy Practices, Acknowledgement of Receipt”
- County of Sacramento HIPAA Form 3013, “HIPAA Privacy & Security Policy & Procedures Acknowledgement Form” or equivalent electronic form
- Division of Behavioral Health Services Acknowledgement of Receipt

Reference(s):

- 45 CFR Parts 160 and 164
- County of Sacramento HIPAA Privacy Rule Policies and Procedures

Policy AS-100-02: Client Privacy Rights

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

CONTENTS

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

The intent of this policy is to set forth and explain the privacy rights that County of Sacramento clients have regarding the use and disclosure of their protected health information (PHI) held by County of Sacramento as guaranteed by HIPAA. This policy shall also establish the procedures the County uses to comply with client privacy rights.

Policy:

County of Sacramento clients have the following HIPAA rights:

1. The Right to Receive a Notice of Privacy Practices

a. County of Sacramento clients have the right to receive a Notice of Privacy Practices written in plain language that explains how the County of Sacramento may use and/or disclose their protected health information, their HIPAA privacy rights, and the County's legal duties with respect to clients' PHI.

b. The County of Sacramento has both healthcare providers and group health plans. The County's Notice of Privacy Practices applies to both providers and plans.

2. The Right of Access to their own PHI, consistent with certain limitations

a. Clients have the right to request access to inspect and/or obtain a copy, or both, of their PHI in a designated record set, as well as to direct the County of Sacramento to transmit a copy to a designated person or entity of the client's choice, consistent with federal law and the California Public Records Law, with some exceptions as shown in the Procedures section.

b. Clients have the right to receive an Accounting of Disclosures that County of Sacramento has made of their PHI, subject to certain limitations as outlined in the Procedure section, for disclosures made up to six years prior to the date of the request for an accounting.

3. The Right to Request an Amendment of PHI that is held by County of Sacramento

a. Clients have the right to request an amendment of their PHI in the designated record set, for as long as the PHI is maintained in the designated record set. Some restrictions apply as shown in the Procedures section.

4. The Right to Request to receive PHI from the County of Sacramento by Alternative Means or at Alternative Locations (Confidential Communications)

a. County of Sacramento health care providers must permit clients to request and must accommodate reasonable requests by clients to receive communications by alternative means, such as by mail, e-mail, fax or telephone; or at an alternative location.

b. County of Sacramento health plans must permit clients to request and must accommodate reasonable requests by clients to receive communications of PHI from the health plan by alternative means or at alternative locations, if the client clearly states that the disclosure of all or part of that information could endanger the client.

5. **The Right to Request Restrictions of the Use and Disclosure of their PHI**

   a. County of Sacramento must permit a client to request restrictions of PHI about the client to carry out treatment, payment or health care operations, and uses and disclosures for involvement in the client's care and notification purposes;

   b. Emergency treatment should be provided even with an agreed upon restriction.

6. **The Right to Submit HIPAA Complaints**

   a. The County of Sacramento has a process for clients to make complaints if they believe or suspect that PHI about them has been improperly used or disclosed, or if they have concerns about the County of Sacramento HIPAA policies and procedures.

   b. The County will document all complaints received and their disposition if any.

7. **The Right to be Notified in the Case of Breach of their unsecured PHI**

   a. The County of Sacramento will notify each individual whose unsecured PHI has been or is reasonably believed by the County to have been accessed, acquired, used or disclosed as a result of a breach.

   b. The effective date of this requirement is applicable to breaches occurring on or after September 23, 2009.

Procedures:

1. **Notice of Privacy Practices**

   County of Sacramento will use the County of Sacramento HIPAA Form 2090, "County of Sacramento Notice of Privacy Practices" to inform clients how the County of Sacramento may use and/or disclose their protected health information (PHI), the client's rights, and the County's legal duties with respect to the client's PHI.

   a. Notice of Privacy Practices for Health Plans

      i. The County of Sacramento health plans must provide a Notice of Privacy Practices:

         A. No later than the compliance date for the health plan, to individuals then covered by the plan;

         B. Thereafter, at the time of enrollment, to clients who are new enrollees; and

C. Must notify clients then covered by the plan no less frequently than once every three years of the availability of the Notice and how to obtain the Notice.

I. The Office of Compliance will coordinate this notification with County of Sacramento Health Plans

II. Notification of availability of the Notice will be made to the named insured of the health plan policy.

D. If there is a material change, the County's health plans must:

I. Prominently post the change or its revised Notice on their websites by the effective date of the material change; and

II. Provide the revised Notice, or information about the material change and how to obtain the revised Notice, in their next annual mailing to the individuals then covered by the plan.

III. In the event the health plan does not post its notice, the health plan must provide the revised Notice, or information about the material change and how to obtain the revised Notice, to clients then covered by the plan within 60 days of the material revision to the Notice.

ii. The County shall prominently post the notice of privacy practices on the Office of Compliance internet website and make the notice available electronically through the website. The website is: http://www.compliance.saccounty.net.

b. Notice of Privacy Practices for Health Providers

i. County of Sacramento health care providers that have a direct treatment relationship with a client shall:

A. Provide the notice:

I. No later than the date of the first service delivery, including service delivered electronically, to such client after the compliance date for the covered health care provider; or

II. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

B. County of Sacramento health care providers that issue the Notice shall make a good faith effort to obtain a signed acknowledgement from each client to document the client's receipt of the Notice of Privacy Practices, If the acknowledgement is not obtained, the provider must document its good faith efforts to obtain the acknowledgment, and why it was not obtained.

I. County of Sacramento will use the County of Sacramento HIPAA Form 2092, "Notice of Privacy Practices Acknowledgement of Receipt" to document the client has received the Notice of Privacy Practices.

A) The Behavioral Health Services Division has its own Acknowledgement of Receipt of the Notice of Privacy Practices incorporated with other acknowledgments required by state law.

II. If client refuses to sign the Acknowledgement of Receipt, the form will be marked accordingly.

III. The original will be placed in the client's medical record or case record file, and a copy given to the client.

ii. County of Sacramento covered health care providers that maintain a physical service delivery site shall:

A. Have the Notice of Privacy Practices available at the service delivery site for individuals to request to take with them;

B. Post the Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice;

C. Whenever the Notice of Privacy Practices is revised, make the Notice available upon request, at the service delivery site; and posted in a clear and prominent location, on or after the effective date of the revision.

D. County of Sacramento will prominently post its Notice on the Office of Compliance website and make the Notice available electronically through its internet website: www.compliance.saccounty.net.

c. Special Requirements for Electronic Notice:

i. County of Sacramento shall prominently post its Notice on the Office of Compliance internet website and make the Notice available electronically: www.compliance.saccounty.net.

ii. The County may provide the notice to a client by e-mail if the client agrees to electronic notice and the agreement has not been withdrawn.

iii. In the event of email failure, paper notice will be provided.

iv. Electronic notice will be provided automatically and contemporaneously in response to an individual's first request for service if that request is made electronically.

v. The individual who is the recipient of the electronic notice retains the right to obtain a paper copy of the notice from the covered entity upon request.

d. County of Sacramento Office of Compliance will maintain and update the Notices of Privacy Practices in accordance with 45 CFR 164.520.

2. Client Request to Access their PHI

County of Sacramento shall ensure that clients may access their PHI that County of Sacramento maintains in the designated record set, and clients may direct the County of Sacramento to transmit a copy to a designated person or entity of the client's choice, subject to certain limitations.

a. Clients may request to inspect and/or obtain a copy, or both, of their PHI.

b. A client's personal representative (generally, a person with authority under State law to make health care decisions for the individual) also has the right to access PHI about the client in a designated record set (as well as to direct the County of Sacramento to transmit a copy of the PHI to a designated person or entity of the individual's choice), upon written request.The requirements shown below apply.

i. All requests for access will be made by having the client complete a County of Sacramento HIPAA Form 2093, "Access to Records Request Form."

A. If the client requests that the County provide access to PHI via unsecured email, and the County is able to provide the PHI via email, the County must comply with this right to access the PHI.

I. In order to provide the client PHI via email the County must obtain from the client the request in writing on HIPAA form 2093 <u>as well as a</u> signed "Consent for PHI to be Sent via Unencrypted Email" form to ensure that the client understands the risks involved in sending PHI via email.

II. The County must send a test email message before sending PHI to the client via email, and must receive a confirmation that the email address is correct.

B. County shall retain Access to Records Requests, Consent for PHI to be Sent via Email forms (if applicable) and the information provided, for 7 years.

ii. County of Sacramento must verify the identity of the individual requesting access by viewing the requestor's valid photo identification or other acceptable types of identification.

A. If the request is received by mail or fax, a copy of the requestor's identification must be included with the Access to Records Request Form.

B. If the person is requesting on behalf of the client as their personal representative, verify the identity and the authority of the person who is requesting access to the PHI.

iii. The County of Sacramento may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate a timely provision of access.

iv. Exceptions to the right of access:

A. Psychotherapy notes;

B. Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding; and

v. Unreviewable Grounds for Denial: The County of Sacramento may deny a client access without providing the client an opportunity for review in the following circumstances:

A. A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

I. NOTE: The denial of an inmate's request applies only to a request to obtain a copy of their records. This does not apply to an inmate's request to inspect PHI. The inmate may designate a personal representative and the personal representative may request a copy of the records on behalf of the inmate.

B. An individual's access to PHI created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

C. An individual's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

D. An individual's access may be denied if the information was obtained from someone other than a health care provider under a promise of confidentiality, and access would reasonably likely to reveal the source of the PHI.

vi. Reviewable Grounds for Denial: County of Sacramento may deny a client access to their PHI, provided that County of Sacramento gives the client a right to have the denial reviewed, in the following circumstances:

A. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the client or another person; or

B. The PHI makes reference to another person (unless the other person is a health care provider), and a licensed health care professional has determined, in the exercise of professional judgment, that the PHI requested may reasonably likely to cause substantial harm to the client or another person; or

C. The request for access is made by the client's personal representative, and a licensed health care professional has determined, in the exercise of professional judgment, that allowing the personal representative to access the PHI may cause substantial harm to the client or to another person.

vii. If County of Sacramento Denies Access:

The client has the right to have the decision reviewed by a licensed health care professional who is designated by the County of Sacramento to act as a reviewing official and who did not participate in the original decision to deny. County of Sacramento will then proceed based on the decision from this review. County of Sacramento must promptly refer a request for review to the designated reviewer. The reviewer must determine, within a reasonable time, whether or not to approve or deny the client's request for access, in accordance with this policy.

A. County of Sacramento must then:

I. Promptly notify the client in writing of the reviewer's determination; and

II. Take action to carry out the reviewer's determination.

B. If the County of Sacramento denies the request, the County will send the requestor the County of Sacramento HIPAA Form 3002, "Denial of Access Form". If County of Sacramento denies access, in whole or in part, to the requested protected health information, County of Sacramento must:

I. Give the client access to any other requested client PHI, after excluding the PHI to which access is denied;

II. Provide the client with a timely written denial using the County of Sacramento HIPAA Form 3002 "Denial of Access Form". The denial must:

A) Be sent or provided within the time limits specified in Section 2.a.viii. of this Procedure, above;

B) State the basis for the denial, in plain language;

C) If the reason for the denial is because obtaining a copy of the PHI would jeopardize the health or safety of the client or another individual, explain the client's review rights as specified in Section 2.a.vii. of this Procedure, above, including an explanation of how the client may exercise these rights; and

D) Provide a description of how the client may file a complaint with County of Sacramento, and if the confidential information denied is protected health information, with the United States Department of Health and Human Services (DHHS) Office for Civil Rights, pursuant to Section 6 of this Procedure, below.

viii. Timely Action. County of Sacramento must act on a client's request for access no later than 30 days after receiving the request.

A. If County of Sacramento grants the client's request, in whole or in part, the County of Sacramento will send the requestor the County of Sacramento HIPAA Form 3003, "Approval of Access Form". This form will inform the client of the access decision and provide the requested access, inspection or copying or both

B. If County of Sacramento maintains the same PHI in more than one format (such as electronically and in a hard-copy file) or at more than one location, County of Sacramento need only provide the requested PHI once.

C. If County of Sacramento is unable to act within the 30 day time period, County of Sacramento may extend the time for action by up to one 30 day extension, subject to the following:

D. County of Sacramento must notify the client in writing within the original 30 time limit of the reasons for the delay and the date by which County of Sacramento will act on the request.

   I. County will retain a copy of notification along with the original request.

E. County of Sacramento will use only one such 30-day extension to act on a request for access.

F. County of Sacramento shall provide the requested PHI in a form or format requested by the client, if readily producible in that form or format. If not readily producible, County of Sacramento will provide the PHI in a readable hard-copy format or such other format as agreed to by County of Sacramento and the client.

G. If County of Sacramento does not maintain, in whole or in part, the requested PHI, and knows where the PHI is maintained, County of Sacramento will inform the client of where to request access.

H. County of Sacramento may provide the client with a summary of the requested PHI, in lieu of providing access, or may provide an explanation of the PHI if access had been provided, if:

   I. The client agrees in advance; and

   II. The client agrees in advance to any fees County of Sacramento may impose, per section 2. J. of this Procedure, below.

I. County of Sacramento must arrange with the client for a convenient time and place for the client and the County of Sacramento to provide access. This may include mailing a copy of the records, having the client pick up a copy of the records, or reviewing records in the County of Sacramento facility.

   I. When the client accesses and reviews the actual health record (not a copy), a staff person must be present at all times.

J. Fees: A client (or legal guardian or custodian) may request a copy of their PHI from the County of Sacramento, which may impose a reasonable, cost-based fee, limited to covering the following:

I. Copying the requested PHI, including the costs of supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; and of the labor of copying the information, whether it is paper or electronic;

II. Postage, when the client has requested or agreed to having the PHI mailed; and

III. Preparing an explanation or summary of the requested PHI, if agreed to in advance by the client.

K. County of Sacramento shall document and retain the client's request to access protected health information, and the reasons for granting or denying the access, in the client's medical record or case record file.

L. County of Sacramento shall document the designated record sets that are subject to access by clients, and the County person or office responsible for receiving and processing the requests for access.

b. Right to Request an Accounting of Disclosures

i. When a client requests an accounting of disclosures that County of Sacramento has made of their PHI, County of Sacramento must provide the client with a written accounting of such disclosures made during the six year period (or lesser time period if specified by the requesting client) preceding the date of the client's request. These accounting of disclosures include disclosures made to or by business associates of the County of Sacramento.

ii. All requests for an accounting of disclosures will be made by having the client complete a County of Sacramento HIPAA Form 2096, "Accounting of Disclosures Request." Requestors are required to show valid photo identification (or other acceptable identification) to make the request.

iii. Examples of disclosures of PHI that are required to be listed in an accounting (assuming that the disclosure is permitted by other confidentiality laws applicable to the individual's confidential information and the purpose for which it was collected or maintained) include:

A. Abuse Report: PHI about an individual provided by County of Sacramento staff (other than protective services staff who respond to such report) pursuant to mandatory abuse reporting laws to an entity authorized by law to receive the abuse report.

B. Audit Review: PHI provided by County of Sacramento staff from an individual's record in relation to an audit or review of a provider or contractor.

C. Health and Safety: PHI about an individual provided by County of Sacramento staff to protect the health or safety of a person.

D. Licensee/Provider: PHI provided by County of Sacramento from an individual's records in relation to licensing or regulation or certification of a provider or licensee or entity involved in the care or services of the individual.

E. Legal Proceeding: PHI about an individual that is ordered to be disclosed pursuant to a court order in a court case or other legal proceeding – include a copy of the court order with the accounting.

F. Law Enforcement Official/Court Order: PHI about an individual provided to a law enforcement official pursuant to a court order – include a copy of the court order with the accounting.

G. Law Enforcement Official/Deceased: PHI provided to law enforcement officials or medical examiner about a person who has died for the purpose of identifying the deceased person, determining cause of death, or as otherwise authorized by law.

H. Law Enforcement Official/Warrant: PHI provided to a law enforcement official in relation to a fleeing felon or for whom a warrant for their arrest has been issued and the law enforcement official has made proper request for the confidential information, to the extent otherwise permitted by law.

I. Media: PHI provided to the media (TV, newspaper, etc.) that is not within the scope of an authorization by the individual.

J. Public Health Official: PHI about an individual provided by County of Sacramento staff (other than staff employed for public health functions) to a public health official, such as the reporting of disease, injury, or the conduct of a public health study or investigation.

K. Public Record: PHI about an individual that is disclosed pursuant to a Public Record request without the individual's authorization.

L. Research: PHI about an individual provided by County of Sacramento staff for purposes of research conducted without authorization, using a waiver of authorization approved by an Institutional Review Board (IRB). A copy of the research protocol should be kept with the accounting, along with the other confidential information required under the HIPAA Privacy Rule, 45 CFR § 164.528(b)(4).

iv. Disclosures that are <u>not</u> required to be tracked and accounted for are those that are:

A. Authorized by the client;

B. Made prior to the original effective date of this policy, which is April 14, 2003;

C. Made to carry out treatment, payment, and health care operations;

D. Made to the client;

E. Made to persons involved in the client's health care;

F. Made as part of a limited data set in accordance with the County of Sacramento Policy AS-100-07**,** "De-identification of Protected Health Information and Use of Limited Data Sets."

G. For national security or intelligence purposes; or

H. Made to correctional institutions or law enforcement officials having lawful custody of an inmate.

v. The accounting must include, for each disclosure:

A. The date of the disclosure;

B. The name, and address if known, of the person or entity who received the protected health information;

C. A brief description of the PHI disclosed; and

D. A brief statement of the purpose of the disclosure that reasonably informs the client of the basis for the disclosure, or, in lieu of such statement, a copy of the client's written request for a disclosure, if any.

vi. If, during the time period covered by the accounting, County of Sacramento has made multiple disclosures to the same person or entity for the same purpose, the County of Sacramento may provide:

A. All of the information identified in Section 2. b. v. of this Section for the first such disclosures; and

B. Identify the frequency, periodicity or number of disclosures made during the accounting period; and

C. The date of the last disclosure made during the accounting period.

vii. County of Sacramento must act on the client's request for an accounting no later than 60 days after receiving the request, subject to the following:

A. If unable to provide the accounting within 60 days after receiving the request, County of Sacramento may extend this requirement by another 30 days. County of Sacramento must provide the client with a written statement of the reasons for the delay within the original 60-day limit, and inform the client of the date by which County of Sacramento will provide the accounting.

B. County of Sacramento will use only one such 30-day extension.

viii. Fees: County of Sacramento must provide the first requested accounting in any 12-month period without charge. County of Sacramento may charge the client a reasonable cost-based fee for each additional accounting requested by the client within the 12-month period following the first request, provided that County of Sacramento:

A. Informs the client of the fee before proceeding with any such additional request; and

Allows the client an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

ix. County of Sacramento will temporarily suspend a client's right to receive an accounting of disclosures that County of Sacramento has made to a health oversight agency or to a law enforcement official, for a length of time specified by such agency or official, if:

A. The agency or official provides a written statement to County of Sacramento that such an accounting would be reasonably likely to impede their activities.

B. However, if such agency or official makes an **oral** request, County of Sacramento will:

I. Document the oral request, including the identity of the agency or official making the request;

II. Temporarily suspend the client's right to an accounting of disclosures pursuant to the request; and

III. Limit the temporary suspension to no longer than 30 days from the date of the oral request, unless the agency or official submits a written request specifying a longer time period.

x. If the individual requests an Accounting of Disclosures that cannot be provided, the County of Sacramento HIPAA Form 3007-B, "Accounting of Disclosures Denial Response" will be sent to the requestor. The following are reasons the Accounting of Disclosures cannot be provided:

A. County of Sacramento has temporarily suspended a client's right to receive an Accounting of Disclosures.

B. The request is for dates prior to April 14. 2003, or for more than six years prior to the date of the request.

C. The individual who made the request is not authorized to receive the Accounting of Disclosures.

D. The individual who made the request did not send a copy of a valid photo identification along with the County of Sacramento HIPAA Form 2096, "Accounting of Disclosures Request Form".

xi. Accounting of Disclosures documentation, including requests and responses, will be maintained in the client's County of Sacramento medical record or case record file, and must be retained for a minimum of 7 years. Documentation should also include the titles of the County person or office responsible for receiving and processing requests for an accounting by individuals.

3. Requesting Amendments of PHI

a. All requests for amendments will be made by having the client complete a County of Sacramento HIPAA Form 2094, "Amendment of Health Records Request Form." Requestors are required to show a valid photo identification (or other acceptable identification) or provide a copy of the identification to verify they have the authority to make the amendment request.

i. If the form is received by mail or fax, a copy of the requestor's identification must be included with the amendment request form.

b. County of Sacramento will honor requests for alternative methods of making this request if reasonable accommodations are needed.

c. County of Sacramento must act on the client's request no later than 60 days of receiving the request. If County of Sacramento is unable to act on the request within 60 days, County of Sacramento may extend this time limit by up to an additional 30 days, subject to the following:

    i. County of Sacramento must notify the client in writing within the 60 day period of the reasons for the delay and the date by which County of Sacramento will act on the receipt; and

    ii. County of Sacramento will use only one such 30-day extension of time for action on the request.

d. If County of Sacramento grants the request, in whole or in part, County of Sacramento must:

    i. Make the appropriate amendment to the PHI or records, and document the amendment in the client's medical record or case record file;

    ii. Identify the records that are affected by the amendment and append or otherwise provide a link to the location of the amendment.

    iii. Provide timely notice to the client using the County of Sacramento HIPAA Form 3005, "Amendment Approval Notification Letter".

    iv. Seek the client's identification of, and agreement to notify the relevant persons or entities, with whom County of Sacramento has shared or needs to share the amended protected health information, of the amendment; and

    v. Make reasonable efforts to inform, and to provide the amendment within a reasonable time to:

        A. Persons named by the client as having received PHI and who thus need the amendment; and

        B. Persons, including business associates of County of Sacramento, that County of Sacramento knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on the information to the client's detriment.

    vi. Prior to any decision to amend a health or medical record, the request and any related documentation shall be reviewed by the program's medical director or a licensed health care professional.

vii. Prior to any decision to amend any other confidential information that is not a health or medical record, a County of Sacramento staff person designated by the program administrator shall review the request and any related documentation.

e. County of Sacramento may deny the client's request for amendment if:

i. County of Sacramento finds the PHI to be accurate and complete;

ii. The PHI was not created by County of Sacramento, unless the client provides a reasonable basis to believe that the originator of such confidential information is no longer available to act on the requested amendment;

iii. The PHI is not part of County of Sacramento designated records set.

f. If County of Sacramento denies the requested amendment, in whole or in part, County of Sacramento must:

i. Provide the client with a timely written denial using the County of Sacramento HIPAA Form 3006, "Denial of Amendment Form". The denial must use plain language and contain:

A. The basis for the denial, as per the reasons in paragraph e., above;

B. The client's right to submit a written statement disagreeing with the denial of all or part of the request for amendment and the basis of such disagreement. The County may reasonably limit the length of a statement of disagreement.

C. A statement that, if the client does not submit a statement of disagreement, the client may request that County of Sacramento provide the client's request for amendment and the denial with any future disclosure of the PHI that is the subject of the amendment; and

D. A description of how the client may file a Complaint to the County of Sacramento, including the name or title, and telephone number of the County person or office designated to receive HIPAA complaints.

I. The Office of Compliance shall receive HIPAA complaints.

g. County of Sacramento shall enter the written statement into the client's County of Sacramento medical record or case record file;

h. County of Sacramento shall also enter a County of Sacramento written rebuttal of the client's written statement into the client's County of Sacramento case record. County of Sacramento will send or provide a copy of any such written rebuttal to the client;

i. County of Sacramento shall include a copy of that statement, and of the written rebuttal by County of Sacramento if any, with any future disclosures of the relevant confidential information. The County may, at its election include an accurate summary of the information with any subsequent disclosure of the PHI to which the disagreement relates; and

j. Explain that if the client does not submit a written statement of disagreement, the client may ask that if County of Sacramento makes any future disclosures of the relevant protected health information, County of Sacramento will also include a copy of the client's original request for amendment and a copy of the County of Sacramento written denial; and

k. Provide information on how the client may file a complaint with County of Sacramento, or with the U.S. Department of Health and Human Services (DHHS), Office for Civil Rights, subject to Section 6 of this Procedure, below.

l. The County of Sacramento, when informed by another covered entity of an amendment to the client's protected health information, must amend the client's PHI in the designated record set in accordance with 45 CFR 164.526 (c)(3).

m. The County of Sacramento shall document the County persons or offices responsible for receiving and processing requests for amendments by clients and retain the documentation for 7 years as required.

n. County of Sacramento will document the client's request, and the reasons for granting or denying the amendment, the client's individual statement of disagreement, and the rebuttal in the client's medical record or case record file.

4. Client's Request for Confidential Communications through Alternative Means or Location

a. County of Sacramento health care providers must permit individuals to request to receive communication of PHI from the provider by alternative means or at alternative locations.

   i. No explanation is required from the client, and the County health care provider may not require an explanation as a condition of accommodating the request.

   ii. The County health care provider must accommodate the request if it is reasonable.

b. Health Plans are subject to slightly different rules. Health Plans must permit individuals to request to receive communication of PHI from the provider by alternative means or at alternative location, if the individual clearly states that the disclosure of all or part of the PHI could endanger the client.

c. The client must specify in writing the preferred alternative means or location. All requests for alternative means or locations will be made by having the client complete a County of Sacramento HIPAA Form 2095, "Restriction of Use and Disclosures/Alternative Communication Request Form."

    i. The County of Sacramento shall verify the identity of the individual making the request. The requester must provide valid photo identification (or other acceptable identification), to verify they have the authority to make the request. If the request is made via mail or fax, a copy of the valid identification must be attached to the request.

d. County of Sacramento will retain the completed County of Sacramento HIPAA Form 2095, "Restriction of Use and Disclosures/Alternative Communication Request Form" in the client's County of Sacramento medical record or case record file for 7 years.

e. Prior to any confidential information being sent to the client, County of Sacramento staff must confirm if the client has requested an alternate location or by alternate means, and if County of Sacramento has granted that request, by reviewing the client's medical record or case record file.

f. County of Sacramento may terminate its agreement to an alternative location or method of communication if:

    i. The client agrees to or requests termination of the alternative location or method of communication in writing. County of Sacramento will document the request in the client's County of Sacramento medical record or case record file.

    ii. County of Sacramento informs the client that County of Sacramento is terminating its agreement to the alternative location or method of communication because the alternative location or method of communication is not effective. County of Sacramento may terminate its agreement to communicate at the alternate location or by the alternative means if:

        A. County of Sacramento is unable to contact the client at the location or in the manner requested; or

        B. If the client fails to respond to payment requests if applicable.

5. Requesting Restrictions of Uses and Disclosures

a. Clients may request that County of Sacramento restrict use and/or disclosure of their PHI for:

   i. Carrying out treatment, payment, or health care operations;

   ii. Disclosure of PHI to a relative or other person who is involved in the client's care.

b. All requests for restrictions will be made by having the client complete a County of Sacramento HIPAA Form 2905, "Restriction of Use and Disclosures/Alternative Communication Request Form." Requestors are required to provide a valid photo identification (or other acceptable identification), to verify they have the authority to make the restriction.

c. County of Sacramento is not required to agree to a restriction requested by the client. The one exception to this rule is;

   i. The County must agree to the client's request to restrict disclosure of PHI to the client's health plan if:

      A. The disclosure is for the purpose of carrying out payment or health care operations and not otherwise required by law; and

      B. The PHI pertains solely to a health care item or service for which the client, or someone on behalf of the client, has paid the County in full.

   ii. County of Sacramento will not agree to restrict uses or disclosures of PHI if the restriction would adversely affect the quality of the client's care or services.

   iii. County of Sacramento cannot agree to a restriction that would limit or prevent County of Sacramento from making or obtaining payment for services.

   iv. Emergency treatment should be provided even with an agreed upon restriction.

      A. **Exception:** For Alcohol and Drug clients, Federal regulations (42 CFR Part 2 and 34 CFR) prohibit County of Sacramento from denying client requests for restrictions on uses and disclosures of their PHI regarding treatment or rehabilitation.

d. County of Sacramento will have all denials for restriction reviewed by a supervisor who may refer to a manager for guidance.

e. County of Sacramento will document the client's request, and the reasons for granting or denying the request, in the client's medical record or case record file. Documentation must be retained for a minimum of 7 years.

   i. Prior to any use or disclosure of client PHI, County of Sacramento staff must confirm that such use or disclosure has not been granted a restriction by reviewing the client's case file.

f. If County of Sacramento agrees to a client's request for restriction, County of Sacramento will not use or disclose confidential information that violates the restriction.

   i. If the restriction is approved, the program area will send the requestor the County of Sacramento HIPAA Form 3000 "Restriction Approval Notification".

      A. **Exception:** If the client needs emergency treatment and the restricted PHI is needed to provide emergency treatment, County of Sacramento may use or disclose such PHI to the extent needed to provide the emergency treatment. However, once the emergency situation subsides County of Sacramento must ask the provider not to further use or disclose the protected health information.

g. If the request is denied, the program will send the requestor the County of Sacramento HIPAA Form 3001, "Restriction Denial Notification"

h. County of Sacramento may terminate its agreement to a restriction if:

   i. The client agrees to or requests termination of the restriction in writing; ~~or~~

   ii. County of Sacramento informs the client in writing that County of Sacramento is terminating its agreement to the restriction. Confidential information created or received prior to notification of termination by the covered entity shall remain subject to the restriction.

   iii. County of Sacramento will document the termination in the client's County of Sacramento medical record or case record file. Documentation shall be retained for 7 years.

6. Filing a Complaint

a. Clients may file complaints with County of Sacramento or with the U.S. Department of Health and Human Services (DHHS) Office for Civil Rights. The Notice of Privacy Practices must provide the name of the County employee or office that can provide clients with information relating to the filing of a complaint with the US Department of Health and Human Services Office for Civil Rights. Such information shall include the address at which the complaint shall be filed.

County of Sacramento:
Office of Compliance
799 G Street #217
Sacramento CA 95814
1-866-234-6883

U. S. Department of Health and Human Services:
Office for Civil Rights
90 Seventh Street, Suite 4-100
San Francisco, CA 94103
1-800-368-1019

b. Clients may file complaints in writing by using the County of Sacramento HIPAA Form 3009, “Privacy Complaint Form”. The form is available on the County Office of Compliance internet: www.compliance.saccounty.net, from the Office of Compliance and from County HIPAA-covered healthcare components. County staff will assist those not able to write the complaint by completing the Complaint Form over the phone or in person.

   i. The complaint must describe acts or omissions believed to be in violation;

   ii. Must be filed within 180 days of the time the complainant knew or should have known of the violation had occurred.

c. County of Sacramento will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.

d. County of Sacramento may not require clients to waive their rights to file a complaint as a condition of providing of treatment, payment, and enrollment in a health plan, or eligibility for benefits.

e. County of Sacramento Office of Compliance shall review and determine action on complaints filed with County of Sacramento. The Office of Compliance shall serve as the point of contact when County of Sacramento is contacted about complaints filed with the U.S. Department of Health and Human Services, Office for Civil Rights.

f. County of Sacramento will send a response to the complaint using the County of Sacramento HIPAA Form 3010, “Complaint Response Form” or equivalent within 30 days of the receipt of the complaint. Complaints may require expedited responses and in some instance require additional time.

g. County of Sacramento will document all complaints, the findings from reviewing each complaint, and County of Sacramento actions resulting from the complaint. This documentation shall include a description of corrective actions that County of Sacramento has taken, if any are necessary, or why corrective actions are not needed, for each specific complaint. This documentation will not include any personnel information regarding County employees. In addition, a copy of the documentation is sent to the Office of Compliance.

h. When responding to a complaint, County of Sacramento will not include PHI to persons who are not the client or legal representative.

i. County of Sacramento will take reasonable efforts to limit the amount of PHI included in the response to the client or legal representative.

j. Complaints can be made anonymously. No responses are provided to anonymous complaints.

k. Complaint documentation must be retained for a minimum of 7 years.

7. The Right to be Notified in the case of Breach of their unsecured PHI

a. The County of Sacramento shall notify each client whose unsecured PHI has been or is reasonably believed by the County to have been accessed, acquired, used or disclosed as a result of a breach.

   i. County of Sacramento HIPAA Privacy Rule Policies and Procedures Policy AS-100-05, Section 2, “Administrative Safeguards”, contains security incident reporting requirements.

b. The effective date of this requirement is applicable to breaches occurring on or after September 23, 2009.

c. A breach shall be treated as discovered by the County of Sacramento as of the first day on which such breach is known, or by exercising reasonable diligence, would have been known to any other person other than the person committing the breach, who is a workforce member or agency of the County of Sacramento.

   i. A HIPAA Risk Analysis will be performed by the Office of Compliance to determine if the incident involves a breach of PHI and is reportable to federal DHHS Secretary as per 45 CFR Subpart D.

   ii. The Office of Compliance will consult with County HIPAA Compliance/Security Officer, County Counsel and/or department management as necessary.

ii. The Office of Compliance will report actual breaches to the federal DHHS Secretary in accordance with 45 CFR Subpart D.

h. Notification to the client. The client whose protected information was breached will be notified by County of Sacramento without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.

i. The Office of Compliance will provide the HIPAA covered component with a Notification Letter template and will assist with the contents of the letter.

ii. The notification shall be written in plain language and include:

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

B. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

C. Any steps clients should take to protect themselves from potential harm resulting from the breach;

D. A brief description of what the County of Sacramento is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

E. Contact procedures for clients to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

iii. The notification will be by first-class mail at the client's last known address. The County of Sacramento will provide notification to the next of kin or personal representative, if the County knows the client is deceased and the County has the address of the next of kin or personal representative.

A. Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the client, a substitute form of notice reasonably calculated to reach the client shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the client.

I. In the case in which there is insufficient or out-of-date contact information for fewer than 10 clients, then such substitute notice may

be provided by an alternative form of written notice, telephone, or other means.

II. In the case in which there is insufficient or out-of-date contact information for 10 or more clients, then such substitute notice shall:

A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the County of Sacramento's website, or may be a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

B) Include a toll-free phone number that remains active for at least 90 days where a client can learn whether the client's unsecured PHI may be included in the breach.

B. Additional notice in urgent situations. In any case deemed by County of Sacramento to require urgency because of possible imminent misuse of unsecured PHI, County of Sacramento may provide information to clients by telephone or other means, as appropriate, in addition to written notice.

i. Notification to the media. Upon discovery of a breach of unsecured PHI involving more than 500 residents of a State or jurisdiction, County of Sacramento shall notify prominent media outlets serving the State or jurisdiction.

i. County of Sacramento shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, unless there is a law enforcement delay.

ii. The notification required shall meet the requirements of 7.i.ii., above.

j. Notification to the Secretary. County of Sacramento Office of Compliance shall, following the discovery of a breach of unsecured PHI notify the federal DHHS Secretary as follows:

i. *Breaches involving 500 or more individuals.* For breaches of unsecured PHI involving 500 or more individuals, County of Sacramento shall except in the event of a law enforcement delay, provide the notification as required by 7.J. above, and contemporaneously with the notice in the manner specified on the federal HHS Website.

ii. *Breaches involving less than 500 individuals.* For breaches of unsecured PHI involving less than 500 individuals, County of Sacramento Office of Compliance shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required for breaches discovered during the preceding calendar year, in the manner specified on the federal HHS website.

k. Notification by a Business Associate. A business associate must notify County of Sacramento of any real or suspected breach involving the County's client's PHI.

   i. Business Associate will supply County of Sacramento with the identification of any client whose PHI has been or suspected to have been breached.

   ii. Business Associate will provide County of Sacramento with any other available information required to include in notification to the client.

l. Law Enforcement Delay. If a law enforcement official states to County of Sacramento that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, County of Sacramento shall:

   i. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

   ii. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in the above paragraph is submitted during that time.

m. Burden of proof. In the event of a use or disclosure in violation of the HIPAA Privacy Rule, County of Sacramento shall have the burden of demonstrating that all notifications were made as required, or that the use or disclosure did not constitute a breach.

Form(s):

- County of Sacramento 2090, "Notice of Privacy Practices"
- County of Sacramento 2092, "Notice of Privacy Practices Acknowledgement Form"
- County of Sacramento 2093, "Access to Records Request Form"
- County of Sacramento 2094, "Amendment of Health Record Request Form"
- County of Sacramento 2095, "Restriction of Use and Disclosures/Alternative Communication Request Form"
- County of Sacramento 2096, "Accounting of Disclosures Request Form"

- County of Sacramento 3000 “Restriction Approval Notification”
- County of Sacramento 3001 “Restriction Denial Notification”
- County of Sacramento 3002 “Denial of Access Form”
- County of Sacramento 3003 “Approval of Access Form”
- County of Sacramento 3005 “Amendment Approval Notification Letter”
- County of Sacramento 3006 “Amendment Denial Notification Letter”
- County of Sacramento 3007 “Accounting of Disclosure Response Form”
- County of Sacramento 3009 “Privacy Complaint Form”
- County of Sacramento 3010 “Complaint Response Form”
- County of Sacramento “Consent for PHI to be Sent via Unencrypted Email” Form

Reference(s):

- 45 CFR Part 160.306
- 45 CFR Part 164.520
- 45 CFR Part 164.522 –164.530
- 45 CFR Subpart D – Breach Notification

Policy AS-100-03: Use and Disclosure of Protected Health Information

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

CONTENTS

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

This policy addresses proper use and disclosure of clients' protected health information (PHI). The County of Sacramento or its business associates (business associate uses and disclosures are addressed in County of Sacramento HIPAA Privacy Rule Policy AS-100-08) may not use or disclose PHI except as permitted or required by HIPAA (45 CFR 164.502) or applicable law, to the authorized and intended recipient. PHI may be accessed by workforce members only for purposes required by the workforce member's assigned job duties. Verification of identity and authority is required for all disclosures. Some uses and disclosures require written authorization by the client; exceptions to this requirement apply under certain circumstances. All uses and disclosures that require the client's authorization shall be documented.

1. Policy: Verification of Identity

Protected health information (PHI) may not be disclosed without verifying the identity and authority of the individual or entity requesting the PHI.

Procedures: Verification of Identity

Examples of requests and identity verification procedures include the following:

a. Request made in person. Individuals may present documents, which normally provide proof of identity, such as employee and military identification cards, driver's license, passport, or other government issued photo identification.

   i. If the individual does not have photo identification, he/she may present two of the following:

      A. Military ID or military discharge papers
      B. Government employee badge
      C. Naturalization papers
      D. Immigration cards
      E. Certified copy of birth certificate
      F. Passport (without a photo)
      G. Check cashing card or food stamp ID card

   ii. HIPAA covered components may follow their program's documented policies and procedures to verify identity and authority.

b. Request by mail, fax or email. Individuals shall provide a copy of photo identification or other identification listed in 1.a.i. above.

c. Third-party request. Individuals are required to furnish a signed authorization granting the third-party access. Examples of third parties who may be requesting records on behalf of the individual include an attorney, an insurance company representative, or a family member or friend of the individual. The request shall include a copy of photo identification or other identification listed in 1.a.i. above.

d. Request by law enforcement. The law enforcement official should present a badge, official identification, or other identification that shows that the official has the authority to accept the PHI on behalf of the law enforcement agency.

e. Request on behalf of a minor. Individuals should provide a copy of a birth certificate, a court order, or other competent evidence of the relationship or authority. In addition, the individual should verify his or her own identity with photo identification.

f. Request by a healthcare provider. The requesting entity should provide the provider's name, facility name, location, and the telephone number.

2. Policy: Use and Disclosure for Treatment, Payment and Health Care Operations (TPO)

a. Protected health information (PHI) may be used or disclosed for treatment, payment and health care operations (TPO) in most cases without the individual's authorization.

   i. Use means the sharing, employment, application, utilization, examination, or analysis of PHI within the entity that maintains the protected health information.

   ii. Disclosure means the release, transfer, provision of access to, or divulging in any other manner, of information outside the HIPAA covered entity holding the PHI.

   iii. **Exception for Psychotherapy notes**: The general rule does not apply to the use and disclosure of psychotherapy notes for treatment, payment or health care operations (TPO). Unless written authorization of the individual is obtained, psychotherapy notes may be used or disclosed for TPO only in very limited circumstances. See Policy 3.a.ii. below for detailed information on psychotherapy notes.

b. Requirements for Using and Disclosing PHI for Treatment, Payment or Health Care Operations (TPO)

   i. Treatment: The covered entity may use or disclose PHI for its own treatment activities. It may disclose PHI for the treatment activities of another health

care provider. The minimum necessary standard does not apply to uses and disclosures for Treatment purposes.

A. Treatment means the provision, coordination or management of health care and related services by one or more health care providers, including:

I. The coordination or management of health care by a health care provider with a third party.

II. Consultation between health care providers relating to a patient; or

III. Referral of a patient for health care from one health care provider to another.

A) Health Care: Health care means care, services, or supplies related to the health of an individual and includes:

(i) Preventative, diagnostic, therapeutic, rehabilitative, maintenance or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body; and

(ii) Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

ii. Payment: As a general rule, PHI may be used or disclosed for a covered entity's own payment activities. A covered entity may disclose PHI to another covered entity or health care provider for the payment activities of the entity that receives the information. The discloser must disclose only the minimum information necessary to accomplish the purpose of the use, disclosure or request.

A. Payment means:

I. The activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or by a health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

II. The activities include, but are not limited to determinations of eligibility or coverage (coordination of benefits or the determination of cost sharing amounts), and adjudication of health benefit claims; risk adjusting amounts; billing, claims management, collection activities, and related health care data processing; review of health care services

with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of certain PHI relating to collection of premiums or reimbursement.

B. No Limitation on Contacts: The Privacy Rule allows disclosure of PHI as necessary to obtain payment. It does not limit to whom disclosures may be made. The County may contact persons other than the client as necessary to obtain payment for health care services.

NOTE: Disclosure of medical information for payment purposes without an authorization is consistent with state law. (Civil Code §56.10(c).)

iii. Health Care Operations: A covered entity may use or disclose PHI for its own health care operations. It may disclose PHI to another covered entity for the health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual, the PHI pertains to such relationship and the disclosure is for quality-related activities or for the purpose of health care fraud and abuse detection or compliance. The discloser must disclose only the minimum information necessary to accomplish the purpose of the use, disclosure or request.

A. Health Care Operations: Health care operations are certain administrative, legal and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. It includes any of the following activities of the covered entity to the extent that the activities relate to covered functions:

I. Conducting quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines) provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;

II. Developing clinical guidelines;

III. Conducting patient safety activities as defined in applicable regulations;

IV. Conducting population-based activities relating to improving health or reducing health care cost;

V. Developing protocols;

VI. Conducting case management and care coordination (including care planning);

VII. Contacting health care providers and patients with information about treatment alternatives;

VIII. Reviewing competence or qualifications of health care professionals;

IX. Evaluating performance of health care practitioners, providers and/or health plans;

X. Conducting training programs or credentialing activities in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers;

XI. Training of non-health care professionals, accreditation, certification, licensing or credentialing activities;

XII. Supporting fraud and abuse detection and compliance programs;

XIII. Except as prohibited under 45 CFR 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance, provided that no genetic information is used or disclosed;

A) A health plan shall not use or disclose genetic information for underwriting purposes.

XIV. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;

XV. Business planning and development;

XVI. Business management and general administrative functions, including but not limited to activities relating to implementation and compliance with the Privacy Rule, customer service, resolution of internal grievances.

Procedures: Use and Disclosure for Treatment, Payment and Health Care Operations

Protected health information (PHI) may be used or disclosed for treatment, payment and health care operations (TPO) without obtaining the client's authorization as written in this section. PHI may only be used or disclosed for purposes permitted or required under the Privacy Rule, and in ways that are permitted or required under the Privacy Rule.

NOTE: Substance abuse programs may not use or disclosure any information about any patient unless the patient has consented in writing or unless another very limited exception specified in the regulations applies. Any disclosure must be limited to the information necessary to carry out the purpose of the disclosure. (42 CFR, Part 2.)

a. Verification of Identity and Authority: County of Sacramento must verify identity, authority and relationship to the client before releasing PHI, including to another provider, biller, or any other party. Disclosures of PHI must be documented in the client's record.

b. Disclosure to the client: County of Sacramento may disclose PHI in a treatment setting to clients who have requested disclosure of their PHI to themselves, or to the client's personal representative, without obtaining written authorization.

   i. County of Sacramento must verify identify the identity of the client or the client's personal representative before discussing PHI in a treatment setting.

   ii. Disclosure of client records is addressed in Section 3 below. Authorization is required.

c. Treatment, Payment and Health Care Operations: County of Sacramento may disclose PHI without authorization for its own treatment, payment or health care operations as authorized by 45 CFR 164.506.

d. Organized Health Care Arrangement: A covered entity that participates in an organized health care arrangement may disclose PHI about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement, unless an exception is noted below.

e. Minimum Necessary Standard: When using or disclosing PHI from or to another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of use, disclosure, or request.

   i. The minimum necessary standard does not apply to use or disclosure of PHI for treatment purposes.

3. Policy: Use and Disclosure of Protected Health Information Requiring Client's Authorization

a. Authorizations

   i. General Rule: Protected health information (PHI) may not be used or disclosed without an authorization, except as otherwise authorized by law. Any use or disclosure pursuant to an authorization must be consistent with the terms of the authorization.

      A. The authorization may be client-initiated or County-initiated. A copy of the signed authorization must be provided to the holder of the PHI. (See Procedures below.)

ii. Psychotherapy Notes: An Authorization for any use or disclosure of psychotherapy notes is required.

A. Psychotherapy notes are notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the client's medical record.

I. Does not include: medication, prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, progress to date.

B. Exception to authorization requirement for psychotherapy notes:

I. To carry out treatment, payment or healthcare operations in the following instances: use by originator of notes for treatment, use/disclosure for training purposes for students, trainees or practitioners in mental health, use/disclosure to defend legal action/other proceeding brought by client.

II. A use/disclosure required by law, for oversight activities, to coroners and medical examiners, if there is a threat to health or safety and to the HHS Secretary to investigate or disclose compliance.

iii. Marketing: An Authorization is required for any use or disclosure of PHI for marketing, except if the communication is in the form of: A face-to-face communication made by a covered entity to an individual; or a promotional gift of nominal value provided by the covered entity.

A. If the marketing involves financial remuneration (direct or indirect payment from or on behalf of a third party whose product or service is being described), to the covered entity, the authorization must state that such remuneration is involved. Direct or indirect payment does not include any payment for treatment of an individual.

iv. Sale of protected health information: An Authorization is required for any disclosure of PHI which is a sale of PHI.

A. Sale of PHI means: A disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

B. A covered entity must obtain an authorization for any disclosure of PHI which is a sale of PHI. (A sale involves direct or indirect payment from or on behalf of a third party to the covered entity. Direct or indirect payment does not include any payment for treatment of an individual.) The authorization must state that the disclosure will result in remuneration to the covered entity.

C. Sale of PHI does not include a disclosure of PHI for any of the following:

I. Public health purposes;

II. Research purposes where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

III. Treatment and payment purposes;

IV. Sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in the definition of health care operations

V. To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

VI. To the client, of their own PHI, when requested;

VII. Required by law; and

VIII. Any other purpose permitted by and in accordance with the applicable requirements, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

v. Valid Authorization: To be valid, an authorization must contain certain information and statements. See Procedures below.

vi. Invalid Authorization: An authorization is not valid if it has any of the following defects:

A. The expiration date has passed or the expiration event is known to have occurred

B. The authorization is not filled out completely with respect to required elements

C. The authorization has been revoked

D. The authorization is an impermissible compound authorization

E. Material information in authorization is known to be false

vii. Compound Authorizations: An authorization cannot be combined with any other document to create a compound authorization; except:

A. Research Study Authorization: An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research related treatment on the provision of one of the authorizations, as permitted, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

B. Psychotherapy Notes: An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

C. Other Exceptions: An authorization, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under this section does not apply to a compound authorization created in accordance with this section.

viii. Revocation of Authorization: An individual may revoke authorization at any time if it is in writing. However, alcohol and drug treatment clients may orally revoke authorization. An authorization cannot be revoked to the extent that

the covered entity has taken action in reliance on the revocation. A revocation does not apply to PHI already released while the authorization was valid and in effect.

NOTE: Although alcohol and drug treatment clients may orally revoke an authorization, the oral revocation must be documented and maintained in the individual's medical record or case record file.

ix. Retention of Authorizations: All HIPAA Authorization forms shall be retained for 7 years in the client's medical record or case record file.

A. Opportunity to Agree or Object

I. General Rule: A covered entity may use or disclose PHI for facility directory purposes and for involving family members or friends in the individual's care, if the individual is informed in advance of the use or disclosure and has the opportunity to agree to, prohibit or restrict the use or disclosure.

ii. Use and Disclosure for Facility Directories: Except when an individual objects, a covered health care provider may:

A. Use the following PHI to maintain a directory of individuals in its facility: individual's name, location in facility, condition (described in general terms) and religious affiliation.

B. Disclose for directory purposes to 1) members of the clergy, all of the above-described PHI; and 2) to all other persons who ask for the individual by name, the individual's general condition and location in the facility.

C. Opportunity to Object: Before using PHI for a facility directory, the health care provider must:

I. Inform the individual that he may be included in the directory and the persons to whom the PHI may be disclosed; and

II. Provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures.

NOTE: Both the notice to the individual and the individual's opt-out or restriction may be given orally, but the agreement or restriction must be documented.

D. Special Circumstances: If it is not practicable to provide an opportunity to object because of an individual's incapacity or any emergency treatment

circumstance, the County may use or disclose some or all of the PHI for the facility directory, if such disclosure is:

I. Consistent with the individual's prior expressed preference, if any, that is known to the County; and

II. In the individual's best interest as determined by the County, in the exercise of professional judgment. Some factors that may be considered include: whether disclosing could reasonably cause harm or danger to the individual (e.g., if it appeared that an unconscious patient had been abused and disclosure could give the attacker sufficient info to seek out and repeat the abuse), whether disclosure of location would give info about the patient's condition (i.e. psychiatric ward), and whether necessary/appropriate to give information about patient status to friends/family (giving info about unconscious patient could help physician determine medications).

III. If the County knows of an incapacitated patient's prior expression of preference, then the County must follow that expression. If there is no known preference, then only the "best interests" portion of the rule governs the discretion of the health care provider. The County may decide to include some portions of the patient's information (name), but not other information (such as location) in order to protect patient's interests.

NOTE: The County must inform the individual and provide an opportunity to object to uses or disclosures when it becomes practicable to do so.

c. Use and Disclosure for Notifying Family or Friends and for Involving Family or Friends in Care

i. General Rule: Subject to an individual's objection or the County's determination that disclosure would not be in best interests of the individual, the County may:

A. Disclose PHI to a person involved with the health care of the client (such as family member, other relative, close personal friend, or any other person identified by the individual).

NOTE: Mental health records regarding a client's diagnosis, prognosis, medication, side effects of medication and client progress may be disclosed to family members only if there is an authorization. (California Welfare & Institutions Code §5328.1.)

I. PHI disclosed must be "directly relevant" to person's involvement with the client's care or payment for the client's health care. No specific definition of "directly relevant" exists in the Privacy Rule, but disclosure should be limited only to the minimum information necessary for the friend or relative to provide the assistance or care s/he was providing.

B. Use or disclosure of PHI to notify or assist in the notification of (including identifying or locating) a family member, a personal representative, or another person responsible for the client's care, of the individual's location, general condition or death.

C. If the client is deceased, a covered entity may disclose PHI to a family member, other relative, or close personal friend, who was involved in the client's care or payment for health care prior to the client's death, that is relevant to such person's involvement, unless doing so is inconsistent with a prior expressed preference of the client that is known to the covered entity.

I. Opportunity to Agree or Object

A) Client Present: If the client is present or available prior to a use or disclosure and has the capacity to make health care decisions, the County may use or disclose PHI only if it:

(i) Obtains the client's agreement to disclose to third parties involved in the client's care;

(ii) Provides the client with an opportunity to object to the disclosure and the client does not express an objection; or

(iii) Reasonably infers from the circumstances, based on professional judgment, the client does not object to the disclosure.

D. Client Not Present/Incapacitated: If the client is not present (e.g., a friend picks up the client's prescription at pharmacy) or the opportunity to agree/object cannot practicably be provided because of the client's incapacity or an emergency circumstance, the County may, in the exercise of professional judgment, determine whether disclosure is in the best interests of the client and disclose only PHI that is directly relevant to the person's involvement with the client's health care.

NOTE: Alcohol and drug treatment programs are not permitted to make this broader disclosure because the medical emergency exception in 42 CFR Part 2 limits disclosure to medical personnel only.

E. Best Interests Considerations: County staff must use professional judgment and must take into account whether disclosure is likely to put the individual at risk of serious harm.

Procedures: Use and Disclosure of Protected Health Information Requiring Client's Authorization

a. Authorizations for County Initiated Use and Disclosure

i. General Rule: Except as otherwise permitted or required by law, County of Sacramento will obtain from the client or the client's personal representative, a completed and signed Authorization for County-initiated release of protected health information (PHI), before obtaining or releasing PHI to or from a third party.

A. The County of Sacramento uses the County of Sacramento HIPAA Forms 2099 and 2099c for this purpose.

I. Form 2099, "Authorization to Obtain or Release Health Records":

Used to obtain or release records when a current treatment relationship is not established, or when a health plan or provider requires an authorization signed by the client, even if for TPO (Treatment, Payment or Operations).

II. Form 2099c, "Authorization to Release Health Records-Multi Disciplinary Team":

Used to release records to members of a Multi-Disciplinary Team (MDT), that includes some team members who are not HIPAA covered, e.g. Probation Officers, Case Workers, etc.

III. Client initiated requests to have their PHI disclosed to a third party of their choosing are addressed in **Policy AS-100-02** under **Client Right to Access**. Client-initiated requests use the County of Sacramento HIPAA Form 2093, "Access to Records Request Form." Client access requests are treated differently than authorizations to obtain or release PHI.

B. County of Sacramento shall provide a copy of the completed, signed form to the client.

C. The original completed and signed form shall be maintained in the HIPAA section of the client's medical record or case record file.

D. Authorization forms shall be retained for 7 years.

ii. Authorizations are initiated by the County to obtain or release client PHI.

iii. Situations requiring a signed authorization:

A. Prior to a client's enrollment in a County of Sacramento administered health plan, if necessary for determining eligibility or enrollment;

B. For the use and disclosure of psychotherapy notes;

C. For disclosures to an employer for use in employment-related determinations;

D. For research purposes unrelated to the client's treatment;

E. For any purpose in which state or federal law requires a signed authorization;

F. For marketing except if the communication is in the form of: face-to-face communication with the client, or a promotional gift or nominal value provided by the County of Sacramento;

I. If the marketing involves financial remuneration to the County, an authorization is required to state that such remuneration is involved.

G. Sale of PHI. An authorization is required for any disclosure involving the sale of PHI;

H. Disclosing PHI when the patient is deceased. A decedent's personal representative (an executor, administrator, or other person who has authority under applicable State or other law to act on behalf of the decedent or the decedent's estate) may access the decedent's PHI.

iv. Valid Authorization: County of Sacramento may obtain, use, or disclose PHI only if the written authorization includes all the required elements of a valid authorization.

A. Uses and disclosures must be consistent with what the individual has authorized on a signed County of Sacramento authorization form.

B. An authorization must be voluntary. County of Sacramento may not require the individual to sign an authorization as a condition of providing treatment services, payment for health care services, enrollment in a health plan, or eligibility for health plan benefits, except:

I. Provisions of health care solely to create PHI for disclosure to third party (e.g., life insurance physical or fitness of duty), prior to enrollment in a health plan if authorization is for the health plan's eligibility or enrollment determinations; or if disclosure is needed to determine payment of claim.

C. County of Sacramento will not ask a client to sign an incomplete authorization form. Authorizations shall be completed only as needed and may not be partially completed and signed by the client "just in case" there is a future need.

D. Forms are required to include the following:

I. The client's name and identifiers in order to ensure the PHI obtained or disclosed is for the correct client.

II. The type of PHI to be obtained or disclosed must be clearly described and must identify the information to be used or disclosed in a meaningful fashion (e.g., discharge summary, laboratory reports, clinical assessments, the entire medical record).

III. An expiration date or event that relates to the client or the purpose of the use or disclosure. The County of Sacramento requires an expiration date of no more than one year from the date the form is signed, and the date must be written on the form.

IV. The name or other specific identification of the person or class of persons authorized to make the requested use or disclosure (e.g., Dr. John Smith, my psychiatrist; the Kaiser Health Plan).

V. A description of each purpose of the requested use or disclosure. The information may not be obtained or disclosed for any purpose other than what is indicated on the form.

A) If the client initiates the release of information, it is sufficient if the purpose indicates "at the request of the individual." No further purpose is required.

NOTE: Client initiated requests to have their PHI sent to a third party of their choosing are addressed in AS-100-02 under Client Right to Access. Client-initiated requests use the County of Sacramento HIPAA Form 2093, "Access to Records Request Form."

VI. The name or other specific identification of the person or class of persons to whom the covered component will obtain or disclose the PHI.

VII. A statement advising that PHI disclosed pursuant to the authorization is subject to redisclosure by the recipient and no longer protected by the Privacy Rule.

VIII. The authorization must advise the client of his right to revoke the authorization in writing and a description of how it may be revoked.

IX. The authorization must advise the client that the County may not condition treatment, payment and/or enrollment in a health plan or eligibility for benefits on signing of authorization by client.

A) **Exceptions**: Provision of health care solely to create PHI for disclosure to third party (life insurance physical, fitness for duty), prior to enrollment in a health plan if authorization is for a health plan's eligibility or enrollment determinations, disclosure is needed to determine payment of claim.

X. A signature and date. If signed by a personal representative of the client, the authorization must contain a description of the representative's authority to act for the individual.

A) A copy of the legal authority or other documentation of the Personal Representative must be attached, if applicable.

B) If the form is faxed or mailed to the County of Sacramento, a copy of the client's (or Personal Representative's) valid photo identification or other acceptable types of identification shall be included and attached to the Authorization form.

XI. Signature and printed name of the County of Sacramento workforce member who assists the client with the form.

vi. Invalid Authorization: An authorization is not valid if it has any of the following defects:

A. The expiration date has passed or the expiration event is known to have occurred;

B. The authorization is not filled out completely with respect to required elements;

C. The authorization has been revoked;

D. The authorization is an impermissible compound authorization;

E. Material information in authorization is known to be false.

vii. Revocation of Authorization: A client may revoke authorization at any time if the revocation is in writing.

NOTE: Alcohol and drug treatment clients may orally revoke authorization; however, the oral revocation must be documented and maintained in the client's case record file.

A. A revocation does not apply to PHI already released while the authorization was valid and in effect.

viii. Opportunity to Agree or Object

A. General Rule: The County of Sacramento may use or disclose protected health information (PHI) for facility directory purposes and for involving family members or friends in the client's care, if the client is informed in advance and given the opportunity to agree or object, and does not object.

B. Oral Agreement: Both the notice to the client, and the client's agreement or objection, may be given orally.

I. County of Sacramento must document and retain any agreed upon use or disclosure or objection to use or disclosure. Documentation shall include the date, what was agreed or objected to, and who or what the restriction is.

A) County of Sacramento may document agreement on County of Sacramento HIPAA Form 2099d, "Client Initiated Release of Health Records" or County of Sacramento HIPAA Form 2093, "Access to Records Request Form," as applicable.

B) County of Sacramento may document objections or restrictions on County of Sacramento HIPAA Form 2095, "Client Request for Restriction/Alternate Communication".

C) Documentation shall be kept in the client's medical record or case record file and retained for 7 years.

C. Individual Present: If the client is present or available prior to a use or disclosure and has the capacity to make health care decisions, the County may use or disclose PHI only if it:

I. Obtains the client's agreement to disclose to third parties involved in the individual's care;

II. Provides the client with an opportunity to object to the disclosure and the client does not express an objection; or

III. Reasonably infers from the circumstances, based on professional judgment, the client does not object to the disclosure.

IV. County of Sacramento must document and retain the agreement. Documentation shall include the date, and what use or disclosure the client agreed to. Documentation shall be kept in the client's medical record or case record file and retained for 7 years.

D. Individual Not Present/Incapacitated: If the client is not present (e.g., a friend picks up the client's prescription at pharmacy) or the opportunity to agree/object cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the County may, in the exercise of professional judgment, determine whether disclosure is in the best interests of the client and disclose only PHI that is directly relevant to the person's involvement with the client's health care.

NOTE: Alcohol and drug treatment programs are not permitted to make this broader disclosure because the medical emergency exception in 42 CFR Part 2 limits disclosure to medical personnel only.

NOTE: All programs will follow their program Policies and Procedures if, in the exercise of professional judgment, the disclosure is in the best interests of the client.

E. Best Interests Considerations: County staff must use professional judgment and must take into account whether disclosure is likely to put the client at risk of serious harm.

4. Policy: Use or Disclosure of Protected Health Information for Other Purposes Not Requiring Authorization

a. General Rule: In some instances, protected health information (PHI) may be used or disclosed, without an authorization and without providing the client with an opportunity to agree or object, for purposes that have been determined to address important goals or needs. Under HIPAA, the following types of uses and disclosures do not require authorization.

i. Uses and Disclosures are Permitted, But Not Required: The uses and disclosures identified in this Policy are permitted, but not required by the Privacy Rule. This means that, in most instances, the County may choose whether to make the use or disclosure without the client's permission; however, some of the disclosures that are only permitted by the Privacy Rule are required by California law. As to those disclosures, the County may not

choose whether or not to make disclosures that are required by California law; it must make those disclosures. On the other hand, some of the disclosures that are permitted by the Privacy Rule are not permitted under California law. **Thus, County staff should determine the County's obligations under state law before making any of the disclosures identified in this Policy.**

ii. Verification Requirements: A covered entity must verify the identity and authority of the persons seeking disclosure of PHI and must obtain any documentation, statements, or representations that the specific provisions of the Privacy Rule governing the disclosure requirement.

A. Disclosure of PHI to Public Official: The County may rely, if such reliance is reasonable under the circumstances, on the following if the disclosure of PHI is made to a public official:

I. If the request is made in person, presentation of an agency identification badge or other credentials or other proof of government status.

II. If the request is in writing, the request is on the appropriate government letterhead; or

III. If the disclosure is to someone acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract or Memorandum of Understanding (MOU).

B. Authority of Public Officials: The County may rely, if such reliance is reasonable under the circumstances, on the following when the disclosure of PHI is to a public official:

I. A written or oral statement of the legal authority under which the information is requested.

II. A warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

iii. Minimum Necessary: The minimum necessary standard applies to all disclosures made without a client's permission except those that are required by law. See Policy AS-100-04 for detailed Information about compliance with the minimum necessary standard.

iv. Documentation: The uses and disclosures authorized without a client's permission must be documented in the client's case record file. Most of the disclosures must be included (logged) in the Accounting of Disclosures that a client may obtain from the County. See Policy AS-100-02 for more information about a client's right to an Accounting of Disclosures.

A. Exceptions–Uses and closures not required to be logged on the Accounting of Disclosures:

I. Made prior to April 14, 2003;

II. Made to carry out treatment, payment, and health care operations;

III. Authorized or made to the client, or to persons involved in the client's health care;

IV. Made as part of a limited data set in accordance with the County of Sacramento Policy AS-100-07, "De-identification of Client confidential information and Use of Limited Data Sets";

V. Made for national security or intelligence purposes; or

VI. Made to correctional institutions or law enforcement officials having lawful custody of an inmate in limited circumstances.

v. Informing the Client: In some cases, the County is required to inform the client of these uses and disclosures. When the requirement exists, the client may be informed orally. The fact that the information was given should always be documented in the client's case record file.

Procedures: Use or Disclosure of Protected Health Information for Other Purposes Not Requiring Authorization

General Rule: In some instances, protected health information (PHI) may be used or disclosed, without an authorization and without providing the client with an opportunity to agree or object, for purposes that have been determined to address important goals or needs.

a. Verification Requirements: A covered entity must verify the identity and authority of the persons seeking disclosure of PHI and must obtain any documentation, statements, or representations that the specific provisions of the Privacy Rule governing the disclosure require. Consult County Counsel for determination about the validity of documentation.

i. Identity of Public Official: The County may rely, if such reliance is reasonable under the circumstances, on the following if the disclosure of PHI is to a public official:

A. If the request is made in person, presentation of an agency identification badge or other credentials or other proof of government status.

B. If the request is in writing, the request is on the appropriate government letterhead; or

C. If the disclosure is to someone acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract or MOU.

ii. Authority of Public Officials: The County may rely, if such reliance is reasonable under the circumstances, on the following when the disclosure of PHI is to a public official:

A. A written or oral statement of the legal authority under which the information is requested;

B. A warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

iii. Documentation: The uses and disclosures authorized without a client's permission must be documented in the client's record. Most of the disclosures must also be listed in the County Accounting of Disclosures Form 2097.

A. Accounting of Disclosures: Some disclosures must be listed on the County Accounting of Disclosures Form 2097. See Policy AS-100-02 for direction on what must be listed on the Accounting of Disclosures.

iv. Minimum Necessary: The disclosures in this section are held to the Minimum Necessary Standard.

b. Disclosures Required by Law

i. General Rule: The County may use or disclose protected health information (PHI) to the extent that such use or disclosure is required by law.

NOTE: HIPAA only requires disclosures under two circumstances: Disclosure to a client of their own PHI, when the client requests the disclosure; or, when required by the Secretary of the federal Department of

Health and Human Services (HHS) to investigate or determine the covered entity's compliance with HIPAA. However, other laws may require disclosures, as stated below.

A. Definition of Required by Law: "Required by law" means a mandate contained in law that compels a use or disclosure of PHI and that is enforceable in court. It includes, but is not limited to: court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers in the program; and statutes and regulations that require the production of information, including statutes and regulations that require such information if payment is sought under a government program providing public benefits.

B. Special Procedures: Specific procedures must be followed when a "required by law" disclosure pertains to any of the following:

I. Disclosures about victims of abuse, neglect or domestic violence that are required by law must be made according to the procedures set forth in Section c.ii. of this section.

NOTE: This does not apply to reports of child abuse or neglect which are considered public health activities.

II. Disclosures for judicial/administrative proceedings that are required by law must be made according to the procedures set forth in Section 3.f. of this section.

III. Disclosures for law enforcement purposes that are required by law must be made according to the procedures set forth in Section 3.g. of this section.

c. Uses and Disclosures for Public Health Activities: PHI may be disclosed for public health activities and purposes.

i. Public Health Authority: PHI may be disclosed without an authorization to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to the reporting of disease, injury, vital events (such as birth or death) and the conduct of public health surveillance, public health investigations and public health interventions. A public health authority may use PHI in all cases in which it would be permitted to disclose PHI for its public health activities.

A. Definition of Public Health Authority: An agency, individual or other entity that is an agency or authority of the United States, a State, a County or a person acting under the grant of authority from such agency and is responsible for public health matters as part of its official mandate. It includes the agency's employees, agents, contractors and other persons or entities to whom the agency has granted authority.

ii. Public Health Authority for Child Abuse Reports: PHI may be disclosed to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect. This is consistent with federal mental health laws.

iii. A Person Exposed to a Communicable Disease: PHI may be disclosed to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation. PHI may be disclosed as needed to notify an individual that he has been exposed to a communicable disease if authorized by law.

iv. An Employer About a Workforce Member in Limited Circumstances: PHI may be disclosed to an employer about a client who is a member of the employer's workforce in limited circumstances.

A. The covered entity is a health care provider that provides the health care service to the client at the request of the client's employer;

B. The health care services provided must relate to the medical surveillance of the workplace or an evaluation to determine whether the client has a work-related illness or injury;

C. The employer must have a duty under OSHA or the requirements of a similar state law, to keep records on or act on such information; and

D. The covered health care provider provides written notice to the client that PHI relating to medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer. The notice may be given either to the client at the time the health care is provided or if the health care is provided at the employer's worksite, by posting the notice in a prominent place at the location where the health care is provided.

v. Immunization Records: A covered entity may use or disclose PHI to a school, about a client who is a student or prospective student of the school, if:

A. The PHI that is disclosed is limited to proof of immunization;

B. The school is required by State or other law to have such proof of immunization prior to admitting the student; and

C. County of Sacramento obtains and documents the agreement to the disclosure from either: A parent, guardian or other person acting in loco parentis of the client, if the client is an unemancipated minor; or from the client, if the student is an adult or emancipated minor.

d. Abuse, Neglect and Domestic Violence: PHI about a client believed to be a victim of adult or dependent adult abuse or neglect or domestic violence may be disclosed to a government authorized by law to receive those reports.

NOTE: Federal mental health laws do not allow disclosure about clients other than children.

i. Special Conditions/Procedures: Disclosures of PHI relating to abuse, neglect and domestic violence must comply with one of the following circumstances:

A. The client agrees to the disclosure, either orally or in writing; or

B. Disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or

C. To the extent the disclosure is expressly authorized by statute or law **and** County of Sacramento, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the client or other potential victims; or if the client is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI being sought is not intended to be used against the client, and that an immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the client is able to agree to the disclosure.

ii. Notice of Disclosure: When any disclosure is made relating to adult abuse, neglect or domestic violence, the client must be promptly informed that the disclosure has been or will be made, except if:

A. Staff, in the exercise of professional judgment and in consultation with appropriate County of Sacramento supervisor, believes that informing the client would place the client or another individual at risk of serious harm; or

B. Staff would be informing a personal representative and County of Sacramento reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the client, as determined by

County of Sacramento, in the exercise of professional judgment and in consultation with appropriate County of Sacramento supervisor.

c. Health Oversight Activities: PHI may be disclosed to a health oversight agency for oversight activities that are authorized by law. The type of oversight activities for which disclosures may be made include audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other actions necessary for appropriate oversight of the health care system, government benefit programs for which health information is necessary for determining compliance with program standards; or entities subject to civil rights laws for which health information is necessary for determining compliance.

NOTE: To the extent that the County or covered entity is also a health oversight agency, it may use PHI for its health oversight activity.

i. Exception: Disclosures may not be made for purposes of an investigation or other activity in which the client is the subject of the investigation or activity and the investigation/activity does not arise out of and is not directly related to either the receipt of health care, a claim for public benefits related to health or qualification for, or receipt of public benefits or services when a client's health is integral to the claim for the benefits or services.

ii. Exception to the Exception: If a health oversight activity/investigation is conducted jointly with an oversight activity/investigation relating to a claim for non-health public benefits, the joint activity/investigation is considered a health oversight activity and disclosure may be made.

f. Judicial and Administrative Proceedings

i. Court Order: PHI may be disclosed in response to an order of a court or administrative tribunal. The PHI must be limited to only that PHI expressly authorized by the order.

ii. Subpoenas, etc.: PHI may be disclosed in response to a subpoena, discovery request, or other lawful process, without a court order, if one of the following circumstances applies:

A. The County receives satisfactory assurances from the party seeking the PHI that reasonable efforts have been made to ensure that the client who is the subject of the PHI has been given notice of the request for PHI; or

B. The County receives satisfactory assurance from the party seeking the PHI that reasonable efforts have been made to secure a qualified protective order.

NOTE: Information that is privileged or confidential under California law should not be disclosed without either the client's authorization or a court order.

g. Law Enforcement Purposes: The County may disclose PHI to a law enforcement official in limited circumstances. A "law enforcement official" means an officer or employee of any agency who has the authority to investigate or conduct an official inquiry into a potential violation of law or to prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law. PHI may be disclosed to a law enforcement official in the following circumstances:

i. When required by law, except laws pertaining to the reporting of child abuse or neglect or other victims of abuse, neglect or domestic violence.

ii. In compliance with a grand jury subpoena, court order or court warrant or an administrative subpoena or demand if the information sought is relevant and material to a legitimate law enforcement inquiry; the request is specific and limited in scope; and de-identified information could not reasonably be used.

NOTE: HIPAA provisions are permissive, not mandatory. Therefore, information that is privileged or confidential under California law should not be disclosed without either the client's authorization or a court order.

iii. If necessary to identify or locate a suspect, fugitive, material witness, or missing person only if the information provided is limited to the following:

A. Name and address

B. Date and place of birth

C. Social security number

D. Blood type and Rh factor

E. Type of injury

F. Date and time of treatment

G. Date and time of death, if applicable

H. Description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos

NOTES: PHI related to the client's DNA or DNA analysis, dental records, or typing samples or analysis of body fluids or tissue may not be disclosed.

The disclosure of this PHI may be made only in response to a law enforcement official's request. It may not be disclosed unless a law enforcement official has asked for it.

Such disclosure is prohibited by federal alcohol and drug laws unless made in a way that does not reveal that the client has a drug/alcohol problem or is in treatment or unless it is made pursuant to an authorization or court order.

iv. About a client who is or is suspected to be a victim of a crime if a law enforcement official requests the information and either

A. The client agrees to the disclosure, either orally or in writing; or

B. If the County of Sacramento is unable to obtain the client's agreement due to incapacity or emergency circumstance, it may disclose PHI if:

I. The law enforcement official represents that such PHI is needed to determine whether a violation of law by someone other than the victim has occurred and such confidential information is not intended for use against the victim;

II. The law enforcement official represents that immediate law enforcement activity would be materially and adversely affected by waiting until the client is able to agree to the disclosure; and

III. County of Sacramento determines that the disclosure is in the best interests of the client.

NOTE: This does not apply to disclosures relating to reports of child abuse and neglect or reports regarding other victims of abuse, neglect or domestic violence.

IV. About a decedent for purposes of alerting law enforcement of the death if it is suspected that the death may have resulted from criminal conduct.

V. If the County believes in good faith that the PHI is evidence of criminal conduct that occurred on the County's premises.

VI. Reporting a crime, while emergency health care, other than relating to an emergency on the County's premises, if disclosure is necessary to alert law enforcement to the commission of a crime, the location of the crime, the victim of the crime and the identity, description and location of the perpetrator.

h. Coroners and Medical Examiners: The County may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. The County may use PHI for those purposes, in accordance with any limitations by state law.

i. Funeral Directors: The County may disclose PHI to funeral directors as necessary to carry out their duties with respect to the decedent. PHI may be disclosed prior to a client's death if necessary for funeral directors to carry out their duties and the client's death is reasonably anticipated.

j. Serious Threats to Health or Safety

i. General Rule: Protected health information (PHI) may be disclosed if all of the following conditions are satisfied:

A. The County in good faith believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a client or the public;

B. The disclosure is made to a person or persons reasonably able to prevent or lessen the threat; and

C. The disclosure is consistent with applicable law and standards of ethical conduct.

ii. Identification of Individual Admitting Violent Crime: PHI may be disclosed if the County in good faith believes the use/disclosure is necessary for law enforcement authorities to identify or apprehend a client who has made a statement admitting participation in a violent crime that the County reasonably believes may have caused serious physical harm and the use/disclosure is consistent with applicable law and standards of ethical conduct.

A. **Exception**: The use/disclosure may not be made if the County learns the information during treatment, counseling or therapy to affect the propensity to commit the criminal conduct or through a request by the client to start such treatment, counseling or therapy.

B. **Limitation**: The only information that may be disclosed is the statement the client made and any of the following identifying/locating information: name and address, date and place of birth, social security number, ABO blood type and Rh factor, type of injury, date and time of treatment, date and time of death if applicable, and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

ii. Identification of Escapee: PHI may be used or disclosed if the County in good faith believes that the use/disclosure is necessary for law enforcement authorities to identify or apprehend a client who has escaped from a correctional institution or from lawful custody, and the use/disclosure is consistent with applicable law and standards.

k. Specialized Government Functions

i. Correctional institutions and other law enforcement custodial situations: PHI may be disclosed about an inmate or other person in lawful custody to a correctional institution or a law enforcement official with lawful custody of the individual, if the official represents that the PHI is necessary for:

A. The provision of health care to the individual;

B. The health and safety of the individual, other inmates;

C. The health and safety of officers, employees or others at the correctional institution or persons responsible for transporting inmates;

D. Law enforcement on the premises of the correctional institution; or

E. The administration and maintenance of the safety, security, and good order of the correctional institution.

NOTE: An individual is no longer an inmate when released on parole, probation, supervised release or when no longer in lawful custody.

ii. Certain covered government programs providing public benefits

A. A health plan that is a government program providing public benefits may disclose PHI relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if a statute or regulation expressly authorizes or requires either a) the sharing of eligibility or enrollment information among agencies; or b) the maintenance of eligibility or enrollment information in a single/combined data system accessible to all the agencies.

B. A covered entity that is a government agency administering a government program providing public benefits may disclose PHI relating to the program to another covered entity that is also a government agency administering a government program providing public benefits if the programs serve the same/similar populations and disclosure of PHI is necessary to coordinate the covered functions or to improve administration and management relating to those functions.

l. Workers Compensation: PHI may be disclosed to the extent necessary to comply with workers compensation laws or laws relating to other similar programs that are established by law and provide benefits for work-related injuries or illness without regard to fault.

NOTE: A client does not have the right to request that a covered entity restrict a disclosure of PHI about them for workers compensation purposes when the disclosure is required by law or authorized by workers compensation.

m. Deceased Individual: A covered entity may use or disclose PHI of a deceased client when the client has been deceased for more than 50 years.

NOTE: California law [Civil Code 56.05(k), 56.35] and federal substance abuse regulations (42 CFR Part 2) continue to apply indefinitely.

Form(s):

- County of Sacramento HIPAA Form 2093, "Access to Records Request Form."
- County of Sacramento HIPAA Form 2095, "Restriction of Use & Disclosures/Alternative Communication"
- County of Sacramento HIPAA Form 2097, "Accounting of Disclosures"
- County of Sacramento HIPAA Form 2099, "Authorization to Obtain/Release Health Records"
- County of Sacramento HIPAA Form 2099c, "Authorization to Release Health Records-Multidisciplinary Team"

Reference(s):

- California Civil Code 56.05(k), 56.35
- 42 CFR Part 2
- 45 CFR Part 164.501
- 45 CFR Part 164.502(a)
- 45 CFR Part 164.506
- 45 CFR Parts 164.508 – 164.512
- County of Sacramento HIPAA Privacy Rule Policy AS-100-02, "Client Rights"
- County of Sacramento HIPAA Privacy Rule Policy AS-100-08, "Business Associates"

Policy AS-100-04: Minimum Necessary Standard

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

The intention of the County of Sacramento Minimum Necessary Standard Policy is to limit the use and disclosure of protected health information (PHI) to that which is necessary to accomplish the intended purpose, limit access to PHI to only workforce members who require access to perform their work duties, and ensure safeguards and practices reflect the minimum necessary standard. (Additional guidance on uses and disclosures is found in Policy AS-100-03, Use and Disclosure of Protected Health Information.)

Policy:

I. General Rule: The minimum necessary requirements in the Privacy Rule require a covered entity such as the designated HIPAA-covered components of County of Sacramento to develop and implement policies and procedures which:

a. Limit uses and disclosures of PHI to the minimum amount of PHI to accomplish the purpose of the use/disclosure;

b. Limit requests for PHI to the minimum amount of PHI to accomplish the purpose of the request; and

c. Limit workforce access to PHI to those authorized users who require the PHI to perform their assigned duties; and

d. Limit workforce access to the PHI required to perform their assigned duties.

2. **Minimum Necessary Rule Not Applicable**: Under the Privacy Rule, the minimum necessary rule does not apply to the following uses or disclosures:

   a. Disclosures to or requests by a health care provider for treatment;

      NOTE: Uses of PHI for treatment are not exempt from the minimum necessary standard.

   b. Uses or disclosures made to the individual who is the subject of the PHI;

   c. Uses or disclosures made pursuant to an authorization that specifies more than the minimum necessary;

   d. Disclosures made to the Secretary of the United States (U.S.) Department of Health and Human Services (DHHS) for compliance enforcement and investigation purposes;

   e. Uses or disclosures required by law;

   f. Uses or disclosures that are required to comply with the Privacy Rule;

      NOTE: For alcohol and drug treatment programs, the minimum necessary standard applies to all disclosures of information.

3. **Minimum Necessary Disclosures of PHI**

   a. Routine and Recurring Disclosures: County of Sacramento must implement policies and procedures regarding any disclosures of PHI that it makes on a routine and recurring basis. The disclosure of PHI must be limited to the amount reasonably necessary to achieve the purpose of the disclosure.

   b. All Other Disclosures: For all other disclosures, County of Sacramento must develop criteria designed to limit the PHI disclosed to that reasonably necessary to accomplish the purpose for which disclosure is sought and review requests on an individual basis in accordance with the criteria.

   c. Reasonable Reliance on Requests for Disclosure: For disclosures of PHI, County may reasonably assume that the minimum necessary standard has been applied when disclosure is requested by public officials, by another covered entity such as a health care provider, and by a professional who is either a member of the workforce or a business associate if the request is to provide services to County of Sacramento and the professional represents that the information requested is the minimum necessary for the stated purpose. Under those circumstances, the covered component of County of Sacramento does not need to make a separate minimum necessary determination.

NOTE: If County staff does not believe that the amount of PHI requested is reasonably necessary for the intended use or purpose staff must attempt to reach a resolution with the requesting party.

d. All disclosures must be documented as per Policy AS-100-03, "Use and Disclosure of Protected Health Information".

4. Minimum Necessary Requests for PHI

a. General Rule: When requesting PHI, County of Sacramento must limit its request to the PHI that is reasonably necessary to accomplish the purpose for which the request is made.

b. Routine and Recurring Requests: County of Sacramento must implement policies and procedures regarding requests for disclosures of PHI that it makes on a routine and recurring basis. The request for PHI must be limited to the amount reasonably necessary to achieve the purpose of the disclosure.

c. Non-Routine Requests (Non-recurring Requests): For all other requests, County of Sacramento must develop criteria designed to limit the PHI requested to that reasonably necessary to accomplish the purpose for which the request is sought and review requests on an individual basis in accordance with the criteria.

Examples: Subpoenas and/or court orders, investigations by law enforcement, abuse, neglect, or domestic violence investigations, Workers' Compensation, regulatory or professional licensure reviews.

5. Use, Disclosure or Request of Entire Medical Record: If the minimum necessary standard applies to a particular use, disclosure or request for PHI, the entire medical record may not be used, disclosed, or requested.

Exception: The covered entity may use, disclose or request the entire medical record if it specifically justifies that the entire record is the amount of PHI that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

Procedure:

The County of Sacramento shall determine if the request is routine or non-routine.

1. Disclosures of an Individual's PHI on a routine or recurring basis:

For routine and recurring disclosures, County of Sacramento shall:

a. Verify the identity and authority of the requestor and the purpose for the request;

i. If the request is **not** compatible with the purpose for which it was collected, refer to and apply the "non-routine use" procedures in the following section.

b. Confirm that the applicable County of Sacramento policies and program rules permit the requested use (disclosure is consistent with the program purposes), and that the nature or type of the use recurs (occurs on a periodic basis) within the program or activity;

c. Identify the type and amount of PHI that is necessary to respond to the request; and

d. If the disclosure is one that must be included in the County of Sacramento **Form 2097**, "Accounting of Disclosures", include required documentation in the client's medical record or case record file.

2. Disclosures of an Individual's PHI on a non-routine basis:

For non-routine disclosures, County of Sacramento shall:

a. Review each request on an individual basis;

b. Verify the identity and authority of the requestor and the purpose for the request;

i. If the request **is** compatible with the purpose for which it was collected, apply the "routine and recurring use" procedures in the previous section.

b. Determine which PHI of the individual is within the scope of the request, and what County of Sacramento policies and program rules apply to the requested use;

c. If the confidential information requested may be disclosed under the applicable program and HIPAA policies, limit the amount of PHI to the minimum amount necessary to respond to the request; and

a. Document the disclosure in the County of Sacramento HIPAA Form 2097, "Accounting of Disclosures" or an equivalent electronic version that incorporates the required elements of the Form 2097.

Form(s):

- County of Sacramento HIPAA Form 2097, "Accounting of Disclosures" or equivalent electronic version.

Reference(s):

- 45 CFR Part 164.502(b), Part164.514(d)
- County of Sacramento HIPAA Privacy Rule Policies and Procedures, Policy AS-100-03, “Use and Disclosure of Protected Health Information”

County of Sacramento HIPAA Privacy Rule Policies and Procedures

Policy AS-100-05: Administrative, Technical and Physical Safeguards

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

CONTENTS

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

The intent of this policy is to implement reasonable and appropriate safeguards to minimize the risk of unauthorized or impermissible access, use or disclosure, in order to protect County of Sacramento's clients' protected health information (PHI).

1. General

County of Sacramento HIPAA-covered components, and business associates, shall implement reasonable safeguards to ensure the confidentiality, integrity and availability of clients' PHI and limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

2. Administrative Safeguards

a. Policies and Procedures

i. The County has written policies and procedures designed to comply with the HIPAA Privacy Rule.

ii. The County shall periodically review and update its HIPAA Policies and Procedures as outlined in the County of Sacramento Security Rule Policies and Procedures Policy 2: "Policy Documentation." The policies and procedures shall be updated periodically to comply with environmental, operational or regulatory changes.

NOTE: If the change materially affects the content of the Notice of Privacy Practice, the County shall promptly revise that notice.

iii. The County of Sacramento's HIPAA Policies and Procedures are accessible to all County of Sacramento workforce members via the Office of Compliance's intranet website: http://inside.compliance.saccounty.net.

b. Risk Analysis, Risk Management, Information System Activity Review, and Evaluation

i. County of Sacramento shall conduct internal reviews to assess the potential risks and vulnerabilities to the confidentiality, integrity, and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the HIPAA-covered components.

ii. HIPAA covered worksites shall receive regular assessments in order to evaluate and improve the effectiveness of current safeguards for PHI.

    A. The Office of Compliance shall conduct site assessments of HIPAA-covered worksites to evaluate the effectiveness of safeguards used in the workplace to protect PHI. The assessments cover Privacy Rule and Security Rule requirements for safeguarding protected health information, incident response and reporting, continuity planning and emergency operations, documentation retention, HIPAA training status, proper retention and destruction of PHI, computer workstation safeguards, work area safeguards, user access management, facility security safeguards, Notice of Privacy Practices, client rights, use and disclosure of PHI, and medical records.

iii. Electronic applications that contain protected health information shall be regularly reviewed to evaluate and improve the effectiveness of current safeguards.

    A. The Office of Compliance shall conduct application assessments of electronic applications that contain ePHI. The assessments cover Security Rule safeguard requirements for user access management, authentication and password management, audit controls, integrity and availability, security incident reporting, contingency plan, and any additional privacy and security features.

iv. The results of the Assessments shall be documented in the appropriate HIPAA Assessment form and shared with the County of Sacramento Privacy Officer, Information Security Officer, and Department and Division management. The Office of Compliance shall maintain the completed Assessment documents.

v. Identified risks shall be communicated to the County HIPAA-covered component to be managed by the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

vi. Additional information can be found in the County of Sacramento HIPAA Security Rule Policies and Procedures Policy 14, “Risk Analysis and Management”.

c. Sanction Policy

i. County of Sacramento shall apply sanctions, including appropriate disciplinary action, against members of the workforce who violate the County's HIPAA Policies and Procedures. All sanctions shall be documented.

A. Workforce sanctions may include suspension or termination of access privileges to PHI; remedial training; appropriate disciplinary action; or personnel actions, up to and including termination of employment. The County's covered component shall determine the appropriate workforce sanction(s).

B. Sanctions may include criminal or civil penalties in accordance with applicable law, as required.

C. Violations of County of Sacramento HIPAA Policies and Procedures may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations, as required.

ii. **Exceptions**: Sanctions do not apply in the following circumstances.

A. Whistleblower: When the member of the workforce (or business associate) discloses PHI while acting as a whistleblower (someone who notifies authorities of the unlawful or unethical actions of the covered entity) and the disclosure is to a health oversight agency or public health authority authorized to investigate or oversee the relevant conduct of the County of Sacramento or to a health care accreditation organization to report alleged failure to meet professional standards or misconduct or to an attorney retained by or on behalf of the workforce member to determine legal options.

B. Workforce Member is Victim of Crime: When the workforce member who discloses PHI is the victim of a crime and disclosure is made about the suspected perpetrator of the criminal act and only certain limited PHI is disclosed.

C. Privacy Complaint: When the workforce member exercises any right under the Privacy Rule, including filing a complaint.

d. Assigned Compliance Responsibility

i. County of Sacramento has a designated privacy official who is responsible for the development and implementation of the County of Sacramento's privacy policies and procedures, and a contact person/office that is responsible for receiving complaints and providing information about matters covered by the required Notice of Privacy Practice.

A. The assigned County of Sacramento privacy official is the County Clerk/Recorder. The Clerk/Recorder may delegate responsibility for the development and implementation of the County of Sacramento's privacy policies and procedures to the Office of Compliance. The Office of Compliance shall be responsible for receiving HIPAA privacy complaints and shall provide information about matters covered by the required HIPAA Notice of Privacy Practice.

e. Workforce Security—Information Access Management

i. County of Sacramento HIPAA-covered components shall ensure that all access to protected health information is role-based access, and shall employ the Minimum Necessary Standard to all access.

A. Role Based Access (RBA) is a form of security allowing access to data based on job function (work role) in accordance with County of Sacramento security procedures. Workforce members shall receive access only to the minimum necessary PHI to fulfill their job functions.

B. Only the application user's manager or an appropriate designee (authorized requestor) shall authorize access to PHI.

C. Workforce members shall receive access only if it is required to perform their assigned job duties.

D. Workforce members shall receive access only to the minimum necessary PHI required to perform their assigned job duties, and shall not access information that is not required for their assigned job duties

E. Access shall be documented and reviewed periodically. Access shall be altered or terminated when the workforce member’s role and responsibilities change, or the workforce member is on a leave of absence, transfers outside of the HIPAA-covered component, or no longer works for the County.

F. The supervisor or manager who is an authorized requestor shall as soon as possible notify Department of Technology to change or terminate computer access.

ii. Additional information can be found in the County’s HIPAA Security Rule Policies and Procedures Policy 3, “User Access Management”.

f. HIPAA Training

i. County of Sacramento's HIPAA-covered workforce is required to be trained in the County of Sacramento's HIPAA policies, procedures and security awareness, as necessary and appropriate for the members of the workforce to carry out their functions within the HIPAA covered component.

ii. All County employee workforce members in HIPAA-covered components shall attend live classroom HIPAA Privacy and Security training within 60 days of assuming a position in a HIPAA covered component, and shall attend re-training at a minimum every two years thereafter, or at a frequency determined by the County Privacy Official.

    A. If web-based HIPAA training is available, all County employees in HIPAA-covered components may attend online HIPAA training, after they have completed the initial live HIPAA training.

iii. Other County workforce members, including employees from temporary agencies, volunteers, registry staff and contractors, shall be trained on the County's HIPAA Privacy and Security Rules, as soon as they are assigned to a HIPAA-covered component.

iv. All workforce members shall sign a County of Sacramento Form 3013 Acknowledgement Form or complete an electronic HIPAA training acknowledgment, attesting to their receipt of County HIPAA Privacy and Security Training, and their compliance with the County's HIPAA Privacy and Security Policies and Procedures.

    A. The Acknowledgement Form will be maintained by the Office of Compliance for a period of seven years.

v. The Office of Compliance shall develop, revise and conduct HIPAA training for the County of Sacramento workforce, and shall document and maintain training records.

vi. Training records and copies of the training materials shall be maintained by the Office of Compliance for a period of seven years.

vii. County of Sacramento departments may have additional training requirements.

viii. County of Sacramento HIPAA Security Rule Policy 15, "Security Awareness and Training" contains additional information.

g. Security Incident and Breach Procedures

    i. Security Incident and Breach Reporting

A. County of Sacramento workforce members are required to report and document all incidents that may affect the privacy, security and integrity of client's PHI. All security incidents, threats to, or violations of, the confidentiality, integrity or availability of PHI shall be reported immediately.

I. A First Report of Incident form may be used to document the facts of the incident.

B. Incidents shall be reported immediately to supervisors or managers. If the supervisor or manager is not available, the incident will be reported immediately by the workforce member.

C. Incidents will be reported to the following:

I. Online at http://createincident.saccounty.net or call 874-5555 for the Service Desk. Please specify that it is a "HIPAA Incident".

II. Send an email to HIPAAOffice@saccounty.net. Include the First Report of Incident.

III. Contact your Division's HIPAA Deputy Compliance Officer.

ii. Incidents to report include, but are not limited to:

A. Suspected or actual unauthorized viewing of PHI or ePHI—including hard copy mail, fax or email sent to incorrect recipient;

B. Unencrypted email that contains PHI;

C. Missing, stolen, lost or damaged paper, or any device that contains PHI, including workstation computer, tablet, netbook, laptop, smartphone, CD, or USB drive;

D. Any unauthorized alteration or corruption of PHI or ePHI;

E. Virus, worm, ransomware, or other malicious code attacks or persistent network or system intrusion attempts from a particular entity;

F. Unauthorized access to PHI, ePHI, or an ePHI based system or network;

G. Unauthorized verbal disclosure;

H. Facility incidents including but not limited to:

I. Unauthorized person found in a HIPAA covered component's facility;

II. Facility break-in;

III. Lost, missing or stolen key, C-Cure badge or cardkey.

iii. The Office of Compliance shall work with the reporting HIPAA covered component and the reporting division Deputy Compliance Officer (DCO) to ascertain all facts and investigate as needed.

iv. In order to evaluate the actions leading up to an incident and to mitigate harm, the responsible HIPAA covered component shall, to the extent practicable, prepare a correction action plan (CAP) that includes reasonable steps taken to reduce the harmful effect of the incident, and prevent further violations.

A. The Office of Compliance may provide guidance with the CAP.

v. The Office of Compliance shall coordinate notification and reporting of all incidents and breaches.

A. In the event of a suspected breach Office of Compliance shall:

1. Notify the County Privacy/Compliance Officer via phone and send an email summary;
2. Notify the DHHS DTech Director and the DTech Information Security Officer of electronic suspected or confirmed breach involving County IT assets, hacking or ransomware;
3. Notify the Division Deputy Compliance Officer.

B. In the event of a confirmed breach, in addition to the above:

1. Notify County Counsel of any serious breach;
2. Notify the appropriate Division or Department manager.

vi. The Office of Compliance shall perform a Risk Analysis to determine if an incident meets the definition of a breach of PHI.

vii. The Office of Compliance shall maintain documentation of reported incidents and breaches for a period of seven years.

viii. County of Sacramento HIPAA Privacy Rule Policies and Procedures Policy AS-100-02, Section 7, “Right to Breach Notification”, contains breach reporting requirements.

h. Contingency Plan

i. The County of Sacramento has a contingency plan for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and nature disaster) that damages systems that contain electronic protected health information (ePHI).

ii. The Contingency Plan is addressed in County of Sacramento HIPAA Security Rule Policies and Procedures Policy 12, “Contingency Plan”.

i. Business Associates

i. County of Sacramento may permit a business associate to create, receive, maintain, or transmit ePHI on behalf of the County of Sacramento only if the County of Sacramento obtains satisfactory assurances that the business associate shall appropriately safeguard the information.

NOTE: Business Associate requirements are addressed in detail in Policy AS-100-08, “Business Associates”.

j. Special Rules for Some Group Health Plans: Group health plans that meet certain conditions are exempt from certain administrative requirements. To qualify for the exemption, the group health plan shall provide health benefits solely through an insurance contract with a health insurance issuer or an HMO and shall not create or receive PHI except for summary health information or information on an individual's participation or enrollment in the health insurance or HMO offered by the plan.

NOTE: Group Health Plans are addressed in detail in Policy AS-100-10, Group Health Plans.

3. Physical Safeguards

a. Facility Access Controls: The County of Sacramento has policies and procedures to limit physical access to its protected health information and the facility or facilities in which it is housed, while ensuring that properly authorized access is allowed.

i. There are safeguards to protect HIPAA-covered facilities and equipment from unauthorized physical access, tampering, and theft.

ii. There are policies and procedures to limit, control and validate a work force member’s access to facilities and worksites based on their role or function, including visitor control.

A. Only authorized workforce members shall enter facilities where protected health information (PHI) is created or maintained. All visitors shall be escorted.

B. Workforce members shall receive the facility and/or worksite access level appropriate to their work role.

C. Only the workforce member’s manager or an appropriate designee (authorized requestor) shall authorize access to facilities or worksites containing PHI.

D. Workforce members shall receive appropriate minimum necessary access level as required to perform their assigned job duties (work role based access).

E. Access shall be altered or terminated when the workforce member's role and responsibilities change, or the workforce member is on a leave of absence, transfers outside of the HIPAA-covered component, or no longer works for the County.

F. The supervisor or manager shall as soon as possible notify Facilities Management or other, as appropriate, to alter or terminate facility access, including disabling C-Cure card access.

G. Workforce members shall keep their C-Cure access card/badge, facility keys and access codes safe and secure at all times, and shall immediately report missing, lost or stolen badge, keys or access codes.

iii. Maintenance records shall be maintained to document when building repairs are requested and completed. The individual responsible for the worksite shall be identified.

A. Metal locks shall be changed when a key is lost or unaccounted for.

iv. "Employee Only" external doors shall be kept shut and locked at all times to prevent unauthorized access.

v. Network/server rooms shall be secured and access to the rooms shall be logged. A HIPAA sign in log shall be maintained in each network/server room in a HIPAA-covered facility.

vi. Records shall be maintained by each HIPAA-covered component of any hard keys, what each key opens, and who keys are issued to. Keys shall be returned when no longer needed by the individual.

vii. Facilities with keypad locks shall change the keypad code every 6 months at a minimum.

viii. Facility access controls are addressed in detail in County of Sacramento HIPAA Security Rule Policies and Procedures Policy 5, "Facility Access Controls".

b. Workstation Use. A workstation is a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

i. County of Sacramento workforce members shall use available safeguards to restrict access by unauthorized users.

A. Workforce members shall make every effort to ensure that confidential information on computer screens is not accessible or visible to unauthorized persons.

I. Computer monitors shall face away from public viewing or a privacy screen shall be used to prevent viewing by unauthorized individuals.

II. Computers shall be set to lock automatically when not in use.

III. Workforce members shall manually lock their computers when away from their workstation by using the Control-Alt-Delete-Enter command or the Windows and L keys.

IV. Workforce members shall never share a log on or password with another individual.

V. Passwords shall not be written down and accessible by unauthorized individuals.

ii. Workstation use is addressed in detail in County of Sacramento HIPAA Security Rule Policies and Procedures Policy 6, “Workstation Security”.

c. Paper

i. County of Sacramento shall ensure that all hard copy (paper) containing PHI is safeguarded from loss or unauthorized use or access.

A. Paper PHI shall be attended or supervised at all times, or secured to prevent unauthorized access, unauthorized viewing, loss or tampering.

B. Each County of Sacramento HIPAA covered workplace shall store files and documents containing protected health information (PHI) in locked rooms or storage systems when the files or documents are not in use and after working hours.

C. In workplaces where lockable storage is not available, County of Sacramento staff shall take reasonable efforts to procure needed lockable storage or use nearby available lockable storage to ensure the safeguarding of PHI.

D. Areas containing paper charts or other written materials with PHI should not be in view of, or easily accessed by, unauthorized individuals. If charts or other documents cannot practicably be kept in a secure area during use, then establish a practice of turning documents over or covering documents to prevent incidental viewing.

E. Materials containing PHI shall not be left in conference rooms, out on desks, or on counters or other areas.

F. A supervisor or manager shall authorize any removal of PHI from the HIPAA-covered worksite and shall document what is removed, who has removed it, and when the PHI is returned.

I. No one shall remove PHI from the worksite without prior approval and authorization.

ii. Transportation of PHI:

A. All PHI in paper and electronic form shall be transported and stored in a secure manner to safeguard it against improper disclosure and/or loss. Confidential information shall be stored or transported outside a secure facility only as necessary. Only the minimum amount of PHI necessary to accomplish the purpose of the use/disclosure should be transported.

B. PHI that is being transported within a facility, such as from one department to another, shall be attended or supervised at all times, and otherwise secured to avoid unauthorized access, loss and/or tampering.

C. Additional measures shall be taken to secure PHI that is being transported outside of a facility to assure confidentiality and integrity in the event of an accident, theft, or other unforeseen event.

iii. PHI that is transported by vehicle:

A. PHI should be transported in a secure container such as a locked box or briefcase whenever possible; and should not be left unattended.

B. PHI should be transported without stops that involve leaving the PHI unattended if possible. If stops must be made do not leave the PHI in the vehicle. Remove it and secure it so that unauthorized individuals cannot access it.

C. Never leave documents or electronic media containing PHI where it can be seen inside an unattended vehicle, even if the PHI is inside a secure container.

D. Do not leave PHI in a car overnight.

iv. Additional measures shall be taken to secure PHI that is taken home or to another location.

A. PHI in the home shall be secured from access or view by family members and others.

B. PHI shall be attended or supervised at all times, or otherwise secured to avoid unauthorized access, loss and/or tampering.

v. PHI that is sent via U.S. Mail or similar delivery system:

A. The sender shall review contents to ensure that the contents are being sent to the correct recipient.

B. Contents shall be sealed in a separate envelope inside, or at the least should have a cover sheet over the contents to prevent incidental viewing by an individual who opens the mail by mistake.

C. The cover sheet shall state the sender's contact information, recipient's name, and a HIPAA Privacy Advisory similar to the advisory in Section 3.c.vii. below.

D. If contents contain PHI on 10 or more individuals, the mail shall be sent Certified, Return Receipt Requested, or an equivalent receipt tracking method.

vi. PHI that is sent via a Courier:

A. The information being transported shall be under the courier's control at all times.

B. The courier shall receive a signed receipt to document that the information was delivered to the correct addressee.

C. The courier shall not leave the information without a signature.

vii. PHI sent via fax:

A. If you share a fax machine, immediately retrieve confidential faxes.

B. Fax machines shall not be located in areas easily accessed by unauthorized persons.

C. Use a fax cover sheet with a Privacy Advisory and contact information in case the fax is received by the wrong person. See sample fax advisory below:

HIPAA PRIVACY ADVISORY

IMPORTANT: This facsimile transmission contains confidential information, some or all of which may be protected health information as defined by the federal Health Insurance Portability & Accountability Act (HIPAA Privacy Rule). This transmission is intended for the exclusive use of the individual or entity to which it is addressed and may contain information that is proprietary, privileged, confidential and/or exempt from disclosure under applicable law.

If you are not the intended recipient, please contact the sender immediately to receive instructions on acceptable methods to permanently destroy the original and any copies of this document.

D. Do not include any PHI on the fax cover sheet.

E. Make sure you send to the correct (intended) recipient:

I. Make sure that the recipient name is correct before you send the fax.

II. Check the fax number to make sure it is correct.

III. If there is any reason to question the accuracy of a fax number, contact the recipient to confirm the number prior to faxing PHI.

F. Review all attachments before sending to ensure the correct information is being faxed.

I. Make sure you have the right number of pages

II. Make sure that the attached pages are the pages you intend to send

III. Look to see if you have accidentally included another client's PHI by mistake!

G. Confirm that the fax was received

I. Make sure the intended recipient knows the fax is coming and retrieves it promptly

II. Follow up to ensure the fax has safely arrived and been received by the intended, authorized recipient.

III. Request a written attestation of destruction if the fax is received by the incorrect recipient.

viii. Disposal

A. Promptly dispose of documents containing protected health information (PHI) that are no longer needed, such as duplicate documents, notes, etc. Place into locked shred bins.

B. If materials containing PHI are in a desk-side temporary shred container, the container shall be emptied into the locked shred bin each day. Temporary shred containers are strongly discouraged.

C. Each County of Sacramento workplace shall ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

D Do not place materials containing PHI into trash bins or recycle bins.

E. Shredding companies: County of Sacramento shall ensure that such entity is under a written contract that requires safeguarding of confidential information throughout the destruction process.

d. Oral:

i. County of Sacramento workforce shall take reasonable steps to protect the privacy of all verbal exchanges or discussions of PHI, regardless of where the discussion occurs, and should be aware of risk levels.

A. Locations of verbal exchange with various risk levels:

I. Low risk: interview rooms, exam rooms, enclosed offices and conference rooms.

II. Medium risk: employee only areas, telephone and individual cubicles.

III. High risk: public areas, reception areas and shared cubicles housing multiple staff where clients are routinely present.

ii. Speak softly when discussing PHI, and be aware of who may be in the surrounding area. Discuss PHI only with individuals you are authorized to disclose the PHI to.

iii. Do not discuss PHI in public areas such as hallways, rest rooms, elevators and reception areas.

iv. Whenever possible use private space when discussing PHI with workforce members, clients, or other authorized individuals.

v. Do not disclose PHI over the phone without verifying the identity and authority of the individual to who you are speaking.

A. Check for restrictions before disclosing PHI over the phone to anyone other than the client.

vi. Do not discuss clients or disclose PHI with anyone, including friends, families or even co-workers, who does not have an authorized, work-related reason to have that information and needs the information in order to perform their assigned work duties.

e. Electronic:

i. County of Sacramento shall ensure that PHI in computers and other portable electronic devices is safeguarded from loss, unauthorized use, access or viewing.

A. Electronic Devices:

I. All access to electronic protected health information (ePHI) shall be authorized as shown in Section 2.e, "Workforce Security—Information Access Management" of this Policy.

II. Workforce members shall not save any PHI on workstation hard drives (also known as the C: \ drive).

III. County of Sacramento shall remove PHI from electronic media before the media is made available for re-use.

IV. County of Sacramento shall maintain an inventory of all portable devices containing PHI, including but not limited to the following: Smartphones, iPhones, iPads and other tablet devices, laptops, USB/flash drives, CDs, DVDs and any other mobile devices, which contain PHI.

V. County of Sacramento shall maintain a record of the movements of hardware and electronic media and the person responsible thereof.

VI. County of Sacramento shall create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

VII. PHI shall not be stored, downloaded or maintained on any portable device without the authorization of the HIPAA-covered component's manager or supervisor.

VIII. Any PHI on a portable device shall be the minimum necessary and shall be deleted after the information has been transferred to and saved on the HIPAA-covered component's assigned network drive or other designated electronic location.

IX. All devices, including County-owned or personally-owned, which are used for County business, shall be password-protected and/or encrypted in accordance with Countywide IT Mobile Device Security Policy.

ii. Email

I. All email containing PHI that is sent outside the County of Sacramento network (@saccounty.net) shall be encrypted.

II. Workforce members may only send PHI via email to authorized recipients.

III. Do not put any PHI into the Subject line of the email.

IV. Check the recipient's names before sending, forwarding or replying to all. Make certain the email is sent only to the correct, authorized recipients.

V. Check and verify new email addresses by sending a test message prior to sending any PHI or confidential information.

a. Use the minimum necessary standard and send only the information that is required for the purpose of the email, and only to the recipients who need that information.

b. If an encryption solution is not available or is not functioning properly use an alternative solution such as faxing.

iii. Multifunction Printer/Copier/Fax Machine

I. Do not send emails containing PHI directly to a recipient from the multifunction copier <u>because they are not encrypted</u> – instead, send the scanned documents to your own email, then send to the intended recipient.

II. New email addresses: send a test message to yourself to make sure the address is entered correctly, and to prevent sending PHI to an unauthorized individual. Do not email any confidential information until the email address is correct.

III. If the multifunction machine does not perform the function requested, such as making copies, stop what you are doing. Check the settings again to verify what action has occurred. Check to see if any accidental transmission has occurred.

IV. Before leaving, make sure that your copy or print job is complete and that no additional functions occurred without your knowledge.

V. Press the "function clear" (or clear function) button before and after each use to prevent the next user from using a function they didn't intend to use.

VI. Use the "Private Print" function if your program has it.

iv. XMedius Fax: Follow the procedures for safe faxing listed above in Section 3. c. vii.

v. HIPAA Security Rule Policy 7: Device and Media Controls address device security in greater detail.

4. Technical safeguards

a. County of Sacramento shall use technical safeguards to limit access to electronic information systems that contain protected health information (PHI) to authorized individuals only, by use of passwords, encryption, anti-virus software and other technical safeguards.

i. Each workforce member who accesses County of Sacramento electronic protected health information (ePHI) shall have a unique user identity.

ii. County of Sacramento shall verify the identity and authority of a person or entity seeking access to the ePHI is the one claimed.

b. Additional Technical Safeguards are addressed in County of Sacramento HIPAA Security Rule Policies and Procedures.

Form(s):

- County of Sacramento HIPAA Form 3013, "HIPAA Training Acknowledgement"
- County of Sacramento HIPAA Site Assessment Form
- County of Sacramento HIPAA Application Assessment Form
- County of Sacramento First Report of Incident Form

Reference(s):

- 45 CFR Part 164.308, Part 164.310 and Part 164.312

- County of Sacramento HIPAA Privacy Rule Policies and Procedures Policies AS-100-02, AS-100-08 and AS-100-10
- County of Sacramento HIPAA Security Rule Policies and Procedures, Policies 2, 3, 5, 6, 9, 12, 14, 15 and 17

Policy AS-100-06: Use and Disclosure for Research Purposes & Waivers of Protected Health Information

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

The intent of this policy is to specify when and how County of Sacramento may use or disclose protected health information (PHI) about individuals for research purposes.

Under HIPAA, research is defined as a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Any project involving PHI where one of the primary goals is generalizable knowledge, with or without publication or public presentation, is considered research.

Policy:

1. General

When County of Sacramento uses or discloses an individual's PHI for research purposes, they must consider the following:

a. County of Sacramento may use or disclose an individual's PHI for research purposes as specified in this policy.

b. All such research disclosures are subject to applicable requirements of state and federal laws and regulations and to the specific requirements of this policy.

Note: This policy is intended to supplement existing research requirements of the Common Rule, 45 CFR Part 46. The Common Rule is the rule for the protection of human subjects in research promulgated by the U.S. Department of Health and Human Services, and adopted by other federal governmental agencies, including the National Institutes for Health, for research funded by those agencies. In addition, some agencies have requirements that supplement the Common Rule that are applicable to a particular research contract or grant.

c. De-identified PHI may be used or disclosed for purposes of research, consistent with County of Sacramento HIPAA Privacy Rule Policy AS-100-07, "De-identification of Protected Health Information and Use of Limited Data Sets."

d. A limited data set may be used or disclosed for purposes of research, consistent with the policies related to Limited Data Sets in Policy AS-100-07.

e. County of Sacramento may also conduct public health studies, studies that are required by law, and studies or analysis related to its health care operations. Such studies will be discussed in Sections 4. and 5. of this Policy.

2. Institutional Review Board (IRB) or Privacy Board established by County of Sacramento

County of Sacramento may use an IRB established in accordance with 45 CFR Part 46, or a Privacy Board that has been established by County of Sacramento pursuant to this policy, to perform the duties and functions specified in this policy regarding a research project being conducted, in whole or in part, by County of Sacramento or by a County of Sacramento office or program.

3. Uses and disclosures for research purposes – specific requirements

a. Individual Authorization: County of Sacramento may use or disclose client PHI for research purposes with the client's specific written authorization.

   i. Such authorization must meet all the requirements described in County of Sacramento HIPAA Privacy Rule Policy AS-100-03, "Uses and Disclosures of Protected Health Information," and may indicate as an expiration date such terms as "end of research study," or similar language.

      Exception: For Alcohol and Drug clients, Federal regulations (42 CFR Part 2) require that a consent form specify the date, event or condition upon which the consent expires, so programs may not use "none" as an expiration date term.

   ii. The authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:

A. An authorization for use and disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study.

I. Includes combining an authorization for the use or disclosure of PHI for a research study with another authorization for the same research study; with an authorization for the creation or maintenance of a research database or repository; or with a consent to participate in research.

B. If research includes treatment, the researcher may condition the provision of research related treatment on the provision of an authorization for use and disclosure for such research.

I. Any compound authorization must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

C. An authorization for use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

D. An authorization, other than an authorization for use or disclosure of psychotherapy notes, may be combined with any other authorization, <u>except</u> when the covered entity has conditioned the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of one of the authorizations. This does not apply to a compound authorization created under A. I. of this section above.

E. An individual may revoke an authorization at any time, provided that revocation is in writing, except to the extent that:

I. County of Sacramento has taken action in reliance to the authorization; or,

II. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or policy itself.

F. County of Sacramento must retain any signed authorization or written revocation for a period of at least seven years.

b. <u>Waivers</u>: County of Sacramento may use or disclose PHI for research purposes <u>without</u> the client's written authorization provided that:

i. County of Sacramento obtains documentation that an alteration to, or waiver, in whole or in part, of an individual's authorization for release of PHI has been approved by either:

   A. An Institutional Review Board (IRB), established in accordance with federal requirements; or

   B. A Privacy Board that:

      I. Has members with varying backgrounds and appropriate professional competency as needed to review the effect of the research protocol on the Individual's privacy rights and related interests;

      II. Includes at least one member who is not affiliated with County of Sacramento, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entities; and

      III. Does not have any member participating in a review of any project in which the member has a conflict of interest.

ii. Documentation required of IRB or privacy board when granting approval of a waiver of an individual's authorization for release of confidential information must include all of the following:

   A. A statement identifying the IRB or privacy board that approved the waiver of an individual's authorization, and the date of such approval;

   B. A statement that the IRB or privacy board has determined that the waiver of authorization, in whole or in part, satisfies the following criteria:

      I. The use or disclosure of an individual's protected confidential information involves no more than minimal risk to the privacy of individuals, based on at least the following elements:

         A) An adequate plan to protect an individual's identifying confidential information from improper use or disclosure;

         B) An adequate plan to destroy an individual's identifying confidential information at the earliest opportunity consistent with the completion of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

C) Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the protected confidential information would be permitted under this policy;

II. The research could not practicably be conducted without the waiver; and

III. The research could not practicably be conducted without access to and use of the individual's PHI;

C. A brief description of the PHI for which use or disclosure has been determined to be necessary by the IRB or privacy board;

D. A statement that the waiver of an individual's authorization has been reviewed and approved under either normal or expedited review procedures, by either an IRB or a privacy board, pursuant to federal regulations at 45 CFR 164.512(i)(2)(iv), Review and Approval Procedures, and

E. The Privacy Board Chair must sign documentation of the waiver of an individual's authorization, or other member as designated by the Chair of the IRB or the Privacy Board, as applicable.

F. County of Sacramento may not require individuals to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits.

c. Reviews Preparatory to Research. A researcher may request access to PHI maintained by County of Sacramento in preparation for research or to facilitate the development of a research protocol in anticipation of research. Before agreeing to provide such access to PHI, County of Sacramento should determine whether federal or state law otherwise permits such use or disclosure without individual authorization or use of an IRB. If there is any doubt whether the use and disclosure of the PHI by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, County of Sacramento will only provide such access if County of Sacramento obtains, from the researcher, written representations that:

i. Use or disclosure is sought solely to review an individual's PHI needed to prepare a research protocol or for similar purposes to prepare for the research project;

ii. No client PHI will be removed from County of Sacramento by the researcher in the course of the review;

iii. The PHI for which use or access is sought is necessary for the research purposes;

iv. Researcher and his or her agents agree not to use or further disclose the PHI other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the PHI other than is provided for by the written agreement;

v. Researcher and his or her agents agree not to publicly identify the PHI or contact the individual whose data is being disclosed; and

vi. Applicable federal or state law may require such other terms or conditions.

d. Research on Decedents Information. A researcher may request access to PHI maintained by County of Sacramento about individuals who are deceased. County of Sacramento should determine whether federal or state law otherwise permits such use or disclosure of PHI about decedents without individual authorization or use of an IRB. There may be instances where it would be inappropriate to disclose PHI, even where the individual subject of the confidential information is dead – for example, individuals who died of AIDS may not have wanted such information to be disclosed after their deaths. If there is any doubt whether the use and disclosure of the PHI by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, County of Sacramento will only provide such access if County of Sacramento obtains the following written representations from the researcher:

i. Representation that the use or disclosure is sought solely for research on the PHI of decedents;

ii. Documentation, if County of Sacramento so requests, of the death of such individuals;

iii. Representation that the PHI for which use or disclosure is sought is necessary for the research purposes.

iv. Researcher and his or her agents agree not to use or further disclose the PHI other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the PHI other than is provided for by the written agreement;

v. Researcher and his or her agents agree not to publicly identify the PHI or contact the personal representative or family members of the decedent; and

vi. Applicable federal or state law may require such other terms or conditions.

4. Public Health Studies and Studies Required by Law

When County of Sacramento is operating as a Public Health Authority, County of Sacramento is authorized to obtain and use PHI without authorization for the purpose of preventing injury or controlling disease, disability and for the conduct of public health surveillance, investigations and interventions. In addition to these responsibilities, County of Sacramento may collect, use or disclose PHI, without individual authorization, to the extent that such collection, use or disclosure is required by law. When County of Sacramento uses PHI to conduct studies pursuant to such authority, no additional individual authorization is required nor does this policy require IRB or privacy board waiver of authorization based on the HIPAA Privacy rules. Other applicable laws and protocols continue to apply to such studies.

5. Studies Related to Health Care Operations

Studies and data analyses conducted for County of Sacramento's own quality assurance purposes and to comply with reporting requirements applicable to federal or state funding requirements fall within the uses and disclosures that may be made without individual authorization as County of Sacramento health care operations. Neither individual authorization nor IRB or privacy board waiver of authorization is required for studies or data analyses conducted by or on behalf of County of Sacramento for purposes of health care operations, including any studies or analyses conducted to comply with reporting requirements applicable to federal or state funding requirements. "Health care operations" as defined in 45 CFR 164.512 include:

a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;

b. Conducting population-based activities relating to improving health care or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with confidential information about treatment alternatives; and related functions that do not include treatment;

c. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, and conducting training programs, and accreditation, certification, licensing or credentialing activities;

d. Underwriting, premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits;

e. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

f. Business planning and development, such as conducting cost- management and planning related analyses related to managing and operating County of Sacramento, including improvement of administration or development or improvement of methods of payment or coverage policies; and

g. Business management and general administrative activities of County of Sacramento, including management activities related to HIPAA implementation and compliance; customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers; resolution of internal grievances; and

h. Creating de-identified confidential information or a limited data set consistent with the County of Sacramento Policy AS-100-07, "De-identification of Protected Health Information and Use of Limited Data Sets."

Exception: HIV-AIDS confidential information may not be disclosed to anyone without the specific written authorization of the individual. Redisclosure of HIV test confidential information is prohibited, except in compliance with law or with written permission from the individual.

6. Accounting of Disclosures for Research Purposes

a. The following information must be included;

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

ii. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

iii. A brief description of the type of PHI that was disclosed;

iv. The date or period of time during which such disclosure occurred;

v. The date of the last such disclosure during the accounting period;

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

vii. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or research activity.

b. The County of Sacramento will assist the individual in contacting the entity that sponsored the research or the researcher at the request of the individual.

Procedure:

Prior to disclosure of PHI, all research projects shall be reviewed by the County's Department of Health and Human Services Research Review Committee.

Form(s):

- County of Sacramento HIPAA Form 2097, "Accounting of Disclosures"

Reference(s):

- 45 CFR Part 64
- 45 CFR Part 164.502, Part 164.508, Part 164.512 and Part 164.528
- County of Sacramento HIPAA Privacy Rule Policy AS-100-02, "Client Privacy Rights"
- County of Sacramento HIPAA Privacy Rule Policy AS-100-07, "De-identification of Protected Health Information and Use of Limited Data Sets"

Policy AS-100-07: De-identification of Protected Health Information and Use of Limited Data Sets

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

The intent of this policy is to prescribe standards under which client protected health information (PHI) can be used and disclosed if information that can identify an individual has been removed (de-identified) or restricted to a limited data set.

Policy:

1. General

a. De-identified information

i. Health information that does not identify an individual, and to which there is no reasonable basis to believe that the information can be used to identify an individual, is not individually identifiable information and therefore is not PHI and not protected by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

ii. Unless otherwise restricted or prohibited by other federal or state law, County of Sacramento can use and share de-identified health information as appropriate for the work of County of Sacramento, without further restriction, if County of Sacramento or another entity has taken steps to de-identify the health information consistent with the requirements and restrictions of this policy in Section 2.

b. Limited Data Set.

i. A limited data set of information may be disclosed to an outside party without a patient's authorization if certain conditions are met. First, the purpose of the disclosure may only be for research, public health or health care operations. Second, the person receiving the information must sign a data use agreement with County of Sacramento, as defined in Section 5, below.

ii. A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers in the limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members.

iii. Because limited data sets may contain identifiable information including dates such as admission, discharge, service, date of birth, date of death, city, state, five digit or more zip code; or ages in years, months or days or hours, which information in combination could lead to the identification of an individual who is the subject of the information, limited data sets are still PHI under the HIPAA Privacy Rule.

iv. County of Sacramento may disclose a limited data set only for the purposes of research, health care operations, or public health purposes. However, the County of Sacramento is not restricted to using a limited data set for its own activities or operations.

A. Where County of Sacramento and a business associate are both governmental entities, County may disclose to the business associate a limited data set to carry out a health care operations function if County has a data use agreement with the business associate.

v. County of Sacramento may use or disclose a limited data set that meets the requirements of Section 4. of this Policy, if County of Sacramento enters into a data use agreement with the limited data set recipient (or with the data source, if County of Sacramento will be the recipient of the limited data set) in accordance with the requirements of Section 5. of this Policy.

vi. If County of Sacramento knows of a pattern or activity or practice of the limited data set recipient that constitutes a material breach or violation of a data set agreement, County of Sacramento will take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, County of Sacramento will discontinue disclosure of confidential information to the

recipient and report the problem to the United States Department of Health and Human Services (DHHS), Office for Civil Rights.

2. Requirements for De-Identification of Client Confidential Information

a. County of Sacramento may determine that client PHI is sufficiently de-identified, and cannot be used to identify an individual, only if **either** i. or ii. below have occurred:

i. A statistician or other person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

A. Has applied such principles and methods, and determined that the risk is minimal that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual who is a subject of the information; and

B. Has documented the methods and results of the analysis that justify such a determination; **or**

ii. County of Sacramento has ensured that:

A. All of the following identifiers of the individual or of relatives, employers, and household members of the individual are removed:

I. Names;

II. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;

III. All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission or discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of “age 90 or older;”

IV. Telephone numbers;

V. Fax numbers;

VI. Electronic mail addresses;

VII. Social security numbers;

VIII. Medical record numbers;

IX. Health plan beneficiary numbers;

X. Account numbers;

XI. Certificate or license numbers;

XII. Vehicle identifiers and serial numbers, including license plate numbers;

XIII. Device identifiers and serial numbers;

XIV. Web Universal Resource Locators (URLs);

XV. Internet Protocol (IP) address number(s);

XVI. Biometric identifiers, including fingerprints and voiceprints;

XVII. Full face photographic images and any comparable images; and

XVIII. Any other unique identifying number, characteristic, or code~~s~~, except as permitted under Section 3. below, of this policy; **and**

B. County of Sacramento has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

b. The County of Sacramento Privacy Officer will designate the statistician or other person referred to in 2.a.i., above, who may be either:

i. A County of Sacramento employee; or

ii. An employee of another governmental agency; or

iii. An outside contractor or consultant, subject to County of Sacramento

contracting and personnel policy.

iv. If not a County workforce member, the individual or entity who performs the de-identification shall be a business associate as per County of Sacramento HIPAA Privacy Rule Policy AS-100-08, “Business Associates”.

3. Re-identification of De-Identified Health Confidential Information

a. County of Sacramento may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by County of Sacramento, provided that:

i. The code or other means of record identification is not derived from or related to confidential information about the individual and cannot otherwise be translated to identify the individual; and

ii. County of Sacramento does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

4. Requirements for a Limited Data Set

a. A limited data set is information that excludes the following sixteen direct identifiers of the individual, or of relatives, employers or household members of the individual:

i. Names;

ii. Postal address confidential information, other than town or city, state and zip code;

iii. Telephone numbers;

iv. Fax numbers;

v. Electronic mail addresses;

vi. Social Security numbers;

vii. Medical record numbers;

viii. Health plan beneficiary numbers (such as Medicaid Prime Numbers);

ix. Account numbers;

x. Certificate/license numbers;

xi. Vehicle identifiers and serial numbers, including license plate numbers;

xii. Device identifiers and serial numbers;

xiii. Web Universal Resource Locators (URLs);

xiv. Internet Protocol (IP) address numbers;

xv. Biometric identifiers, including finger and voice prints; and

xvi. Photographic image of a person's face which would allow identification by sight or electronic means.

5. Contents of a Data Use Agreement

a. County of Sacramento may use or disclose a limited data set only if County of Sacramento obtains satisfactory assurance, in the form of a data use agreement in accordance section 5.b. immediately below, that such entity will use or disclose the protected health information only as specified in the written agreement.

b. A data use agreement between County of Sacramento and the recipient of the limited data set shall:

i. Specify the permitted uses and disclosures of such information by the limited data set recipient. The data use agreement may not permit the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this Policy.

ii. Specify who is permitted to use or receive the limited data set; and

iii. Specify that the limited data set recipient will:

A. Not use or further disclose the information other than as specified in the data use agreement or as otherwise required by law;

B. Use appropriate safeguards to prevent use or disclosure of the confidential information other than as specified in the data use agreement;

C. Report to County of Sacramento, if the recipient becomes aware of any use or disclosure of the information not specified in its data use agreement

with County of Sacramento;

D. Ensure that any agent, including a subcontractor, to whom it provides the limited data set, agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

E. Not identify the information or contact the individuals whose data is being disclosed.

6. Limited Data Set Compliance

a. County of Sacramento is not in compliance if the County knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the County took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

   i. Discontinued disclosure of protected health information to the recipient; and

   ii. Reported the problem to the federal DHHS Secretary.

b. If the County of Sacramento is a limited data set recipient and violates a data use agreement, the County will be in noncompliance with the standards, implementation specifications, and requirements of 45 CFR 164.514 (e)(4)(iii).

Reference(s):

- 45 CFR 164.514
- County of Sacramento HIPAA Privacy Rule Policy AS-100-08, “Business Associates”

Form(s):

- None

Policy AS-100-08: Business Associates

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

This policy addresses applicability and responsibilities of business associates (BAs), and includes the 2013 Omnibus Rule provisions. BAs are directly subject to the HIPAA penalties for non-compliance. BAs must comply with the Security Rule and with sections of the Privacy Rule. BAs must ensure their subcontractors also comply with the HIPAA requirements.

Policy:

1. General

a. HIPAA regulations require that covered entities enter into contracts ("Business Associate Agreements", or BAA) with their BAs to ensure that the BAs will appropriately safeguard protected health information (PHI). The BAA also serves to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by the BA, based on the relationship between the parties and the activities or services being performed by the BA. A BA may use or disclose PHI only as permitted or required by its BAA or as required by law.

   A BA is directly liable under HIPAA regulations and subject to civil and, in some cases, criminal penalties for making uses and disclosures of PHI that are not authorized by the BAA or required by law. A BA also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

b. If a contractor or business partner is a BA, those contracts that define the contractual relationship remain subject to all federal and state laws and policies governing the contractual relationship. A BA relationship also requires additional contract provisions. The additional contract requirements are described in Section 2 below.

c. BA meaning (per 45 CFR §160.103):

A "business associate" (BA) is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the BA to protected health information (PHI). A BA also is a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another BA.

A BA relationship is formed only if PHI is used, created, maintained or transmitted in the relationship. The following are BA functions, activities or services:

i. BA functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. ii. BA services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

ii. The following types of organizations are included in the definition of business associate:

A. A Health Information Organization, E-prescribing Gateway, or other person or organization that provides data transmission services with respect to PHI to the County of Sacramento and that requires routine access to such PHI; and

B. A person or entity who offers a personal health record to one or more clients on behalf of the County of Sacramento.

iii. A covered entity participating in an organized health care arrangement that performs a function or activity as described in i.A. of this definition or that provides a service as described in i.B. of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a BA of other covered entities participating in such organized health care arrangement.

iv. A covered entity may be a BA of another covered entity.

d. The following are **not** BAs or BA relationships:

   i. County of Sacramento employees, offices, and programs which are part of the covered components of the County;

   ii. Medical providers exclusively providing treatment to clients;

   iii. Enrollment or eligibility determinations, involving County of Sacramento clients, between government agencies;

   iv. Payment relationships, such as when County of Sacramento is paying medical providers, child care providers, managed care organizations, or other entities for services to County of Sacramento clients, when the entity is providing its own normal services that are not on behalf of County of Sacramento;

   v. When a client's protected health information is disclosed based solely on a client's authorization;

   vi. When a client's PHI is not being disclosed by County of Sacramento or created for County of Sacramento; and

   vii. When the only information being disclosed is information that is de-identified in accordance with County of Sacramento Privacy Rule Policy AS-100-07, "De-identification of Protected Health Information and Use of Limited Data Sets."

e. County of Sacramento may disclose a client's PHI to a BA and may allow a BA to create, receive, maintain or transmit a client's PHI on behalf of County of Sacramento, if:

   i. County of Sacramento first enters into a written contract, or other written agreement or arrangement, with the BA before disclosing a client's PHI to the BA, in accordance with the requirements of Section 2, below, of this policy.

   ii. The written contract or agreement provides satisfactory assurance that the BA will appropriately safeguard the information.

f. A BA may permit their subcontractor to create, receive, maintain, or transmit electronic protected health information (ePHI) on its behalf only if the BA obtains satisfactory assurances, in accordance with 45 CFR 164.314(a), that the subcontractor will appropriately safeguard the information. (See Section 2, "Contract Requirements", below.)

g. County of Sacramento is not required to obtain such satisfactory assurances from a BA that is a subcontractor of the County's BA.

2. Contract Requirements Applicable to Business Associates (BAs)

a. A contract or other arrangement between County of Sacramento and a BA must include terms and conditions that:

i. Establish the permitted and required uses and disclosures of protected health information (PHI) by the BA. The contract may not authorize the BA to further use or further disclose PHI obtained from County of Sacramento, except that the contract may permit the BA to:

A. Use and disclose protected confidential information for the proper management and administration of the business associate; and

B. Collect data relating to County of Sacramento health care operations.

ii. Provide that the BA shall:

A. Not use or further disclose PHI other than as permitted or required by the contract or as required by law;

B. Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by the contract;

C. Report to County of Sacramento any use or disclosure not allowed by the contract of which the BA becomes aware, as required by state and federal regulations including breaches of unsecured PHI, and any security incident of which it becomes aware;

D. Ensure that any agents or subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same restrictions, conditions and requirements that apply to the BA under the contract with County of Sacramento, by entering into a contract or other arrangement with the BA;

E. Make PHI in a designated record set available to the client in accordance with County of Sacramento HIPAA Privacy Rule Policy AS-100-02, “Client Privacy Rights;”

F. Make PHI in a designated record set available for amendment and incorporate any amendments in accordance with County of Sacramento HIPAA Privacy Rule Policy AS-100-02, “Client Privacy Rights;”

G. Maintain and make available the information required to provide an accounting of disclosures in accordance with County of Sacramento HIPAA Privacy Rule Policy AS-100-02, “Client Privacy Rights;”

H. Makes its internal practices, books, and records relating to the use and disclosure of protected health information available to County of Sacramento and to the United States Department of Health and Human Services (DHHS) for the purpose of determining County of Sacramento compliance with federal requirements; and

I. At termination of the contract, if reasonably feasible, the BA shall recover any PHI relating to the contract in the possession of its subcontractors, agents or representatives. The business associate shall return to County of Sacramento, or destroy with consent of County of Sacramento, all such protected health information plus all other protected health information relating to the contract and in its possession and shall retain no copies. If not feasible, the BA shall continue to protect the confidential information.

iii. Authorize termination of the contract if County of Sacramento determines that the BA has violated a material term of the contract unless inconsistent with the County's statutory obligations.

b. If the BA of County of Sacramento is another governmental entity:

i. County of Sacramento may enter into a memorandum of understanding (MOU), rather than a contract, with the BA if the MOU contains terms covering all objectives of 2.a. above, of this policy;

ii. The written contract, agreement, or MOU does not need to contain specific provisions required under 2.a. above, if other law or regulations contain requirements applicable to the BA that accomplish the same objective;

c. If a BA is required by law to perform a function or activity on behalf of County of Sacramento, or to provide a service to County of Sacramento, County of Sacramento may disclose PHI to the BA to the extent necessary to enable compliance with the legal requirement, without a written contract or agreement, if:

i. County of Sacramento attempts in good faith to obtain satisfactory assurances from the BA that the BA will protect confidential information to the extent specified in 2.a., above; and

ii. If such attempt fails, County of Sacramento documents the attempt and the reasons that such assurances cannot be obtained;

d. Other requirements for written contracts or agreements: The written contract or agreement between County of Sacramento and the BA may permit the BA in its capacity as a BA necessary to:

i. Use and disclose confidential information it receives in its capacity as a BA if:

A. The disclosure is required by law; or

B. The BA receives reasonable assurances from the person to whom the confidential information is disclosed that:

I. It will be held or disclosed further only as required by law or for the purposes to which it was disclosed to such person; and

II. The person notifies the BA of any known instances in which the confidentiality of the confidential information has been breached.

ii. Use information for the proper management and administration of the BA; or

iii. Use information to carry our legal responsibilities of the BA, provided the disclosures are required by law, or the BA obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies BA of any instances of which it is aware ~~that~~ the confidentiality of the information has been breached.

3. Omnibus Rule Transition

1. New business associates must comply with the Omnibus Rules provisions as of March 26, 2013.

2. New and renewing business associate agreements must have the new Business Associate Agreement in place.

3. "Grandfathered": Valid business associate agreements in place as of January 25, 2013 have until September 23, 2014 to be updated:

a. As long as it's not renewed or modified between March 26, 2013 and September 23, 2013; and

b. Will be compliant until the earlier of

The date the business associate agreement is renewed or modified on/after September 23, 2013; or September 22, 2014.

4. Deadline: All covered entities and business associates must comply with the Omnibus Rule's provisions by September 23, 2013.

Procedure:

1. Tracking and identifying County of Sacramento Business Associates (BAs)

a. County of Sacramento will identify those business relationships that are also BAs.

   i. Contracts staff will complete the County of Sacramento HIPAA Form 3011, "Business Associate Decision Tool" as part of the contract approval process.

   ii. The contract will be forwarded to County Counsel along with the Business Associate Decision Tool.

   iii. County Counsel will review the Business Associate Decision Tool with the contract and accompanying documents to make a determination if a contractor is a BA as defined in the Health Insurance Portability and Accountability Act (45 CFR 160.103).

b. If County Counsel determines that the contractor is a BA then the contract documents shall include a Business Associate Agreement (BAA) and the BA Requirements paragraph in the contract agreement, as described in Appendix L, Standard Form Agreement, Section XXIV, "Business Associate Requirements," of the County Contract Manual found on County Counsel's web site.

c. County of Sacramento will include legally appropriate BA contract terms and conditions in such contracts, which may include incorporation by reference to administrative rule.

d. Contract staff will document the HIPAA business relationship information provided to them by the Contract Requestor at the time the request is received.

   i. Contracts staff will keep a list of all identified BAs and provide the list to the Office of Compliance at a minimum twice yearly.

   ii. The Office of Compliance will review and maintain copies of the list of BAs.

2. Responsibilities of County of Sacramento in Business Associate (BA) Relationships

a. County of Sacramento will provide BAs with applicable contract requirements, as needed, on how to comply with contract requirements regarding protected health information (PHI).

b. The County may also be a BA of another covered entity if the County is performing any of the activities described in Section 1.c. Before the County signs any business associate agreement (BAA) submitted by the other covered entity, County Counsel shall review and approve that agreement.

c. County of Sacramento responsibilities in BA relationships include, but are not limited to, the following:

i. Receiving and logging a client's complaints regarding the uses and disclosures of PHI by the BA or the BA relationship;

ii. Receiving and logging reports from the BA of possible violations of the BA contracts;

iii. Implementation of corrective action plans, as needed; and

iv. Mitigation, if necessary, of known violations up to and including contract termination.

3. Business Associate (BA) Non-Compliance

a. If County of Sacramento knows of a pattern of activity or practice of a BA that constitutes a material breach or violation of the BA's obligation under the contract or other arrangement, County of Sacramento must take reasonable steps to cure the breach or end the violation, as applicable, including working with and providing consultation to the BA.

b. If such steps are unsuccessful, County of Sacramento must:

i. Terminate the contract or arrangement, if feasible; or

ii. If termination is not feasible, report the problem to the United States Department of Health and Human Services (DHHS).

4. County of Sacramento's Response to Complaints about Business Associates (BAs) Inappropriate Uses or Disclosures

a. County of Sacramento staff who receives a client complaint, or a report or complaint from any source, about inappropriate uses or disclosures of confidential information by BAs, shall

i. Provide confidential information regarding that report or complaint to the County of Sacramento Office of Compliance, who will document the complaint.

b. The County of Sacramento Office of Compliance will coordinate with the BA's County of Sacramento contract administrator to document the alleged violation.

c. The County of Sacramento contracts staff will send a letter to the BA, requesting that the BA review the circumstances related to the alleged pattern or practice. County of Sacramento will require that the BA respond, in writing, within 10 business days to the complaint.

i. If determined necessary and appropriate, County of Sacramento contracts staff will generate a “cure letter” outlining required remediation in order for the BA to attain contract compliance.

d. County Counsel shall be contacted and consulted in the event of non-compliance with HIPAA BA provisions.

e. Where contract compliance cannot be attained, County of Sacramento must terminate the contract, if feasible. If termination is not feasible, the County of Sacramento Privacy Officer will report the problem to the United States DHHS, Office of Civil Rights.

5. Notification of Breach

a. As required by 45 CFR Section 164.308(a)(2), the BA shall notify County of Sacramento in writing within five (5) working days of its discovery of any use or disclosure of PHI not permitted by the agreement of which the BA or its officers, employees or agents become aware. Such notice shall include the name of each client, with address or other identifiers where known, whose unsecured PHI has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such unauthorized use or disclosure.

b. Any unauthorized use or disclosure shall be treated as discovered by the BA on the first day on which such access, acquisition or disclosure is known to the BA, including any person, other than the individual committing the unauthorized use or disclosure, that is an employee, officer or other agent of the BA, or who should reasonably have known such unauthorized activities had occurred.

c. BA shall promptly identify, respond to and report to County any suspected or known "security incident" of which it becomes aware. Such term is defined in the HIPAA Security Rule, 45 CFR Section 164.304: “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” BA’s incident report shall identify the date of the security incident, the scope of the security incident, the BA's response to the security incident and the identification of the party responsible for causing the security incident, if known.

d. BA agrees that any sub-contractor of the BA that provides services to the BA has the same responsibilities regarding reporting unauthorized uses or disclosures as the BA. BA shall ensure that these responsibilities are defined in any sub-contract it enters into in order to service an agreement with the County of Sacramento.

e. The County of Sacramento Office of Compliance will coordinate with the BA’s County of Sacramento contract administrator to:

i. Document the breach;

ii. Notify affected client(s);

iii. Notify the DHHS Secretary; and

iv. Notify major media if the breach involves more than 500 residents of a State or jurisdiction.

Reference(s):

- 45 CFR §160.103, §164.304, §164.308, §164.314, §164.402, §164.504 and §164.410

Form(s):

- County of Sacramento HIPAA Form 3011, “Business Associate Decision Tool”
- County of Sacramento Business Associate Agreement, also known as Appendix N, Contract Boilerplate HIPAA Provision
- County of Sacramento Contract Manual Section XXIV, “Business Associate Requirements”, County of Sacramento Appendix L Standard Form Agreement

Policy AS-100-09: Enforcement, Sanctions and Penalties

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

The intent of this policy is to specify enforcement, sanction, penalty, and disciplinary actions that may result from violation of County of Sacramento policies regarding the privacy and protection of an individual's protected health information and to offer guidelines on how to conform to the required standards.

Policy:

1. General

a. The County of Sacramento must have and apply appropriate sanctions against its workforce members who fail to comply with the County's HIPAA policies and procedures. These sanctions do not apply to disclosures by whistleblowers and workforce member crime victims.

b. All County of Sacramento workforce members in HIPAA-covered components (including employees, contract employees, temporary agency employees, registry employees, volunteers, and interns), and County of Sacramento's business associates, must guard against improper uses or disclosures of a County of Sacramento client's protected health information.

i. County of Sacramento workforce members, who are uncertain if a disclosure is permitted, shall consult with a supervisor in the County of Sacramento workplace. County of Sacramento Office of Compliance is a resource for any County of Sacramento HIPAA-covered component that cannot resolve a disclosure question, and may be consulted in accordance with the operational procedures of that County of Sacramento component.

c. All workforce members are required to be aware of their responsibilities under County of Sacramento HIPAA Privacy Rule and Security Rule policies and procedures.

i. County of Sacramento workforce members will be expected to sign a County of Sacramento HIPAA Privacy & Security Acknowledgement Form 3013, or an electronic equivalent, indicating that they have received training on the County's HIPAA Privacy and Security Rule policy and procedures and they understand their responsibilities to comply with the HIPAA Privacy and Security Policies and Procedures to ensure the privacy of County of Sacramento clients' protected health information (PHI).

.

d. Supervisors are responsible for assuring that workforce members who have access to PHI, in any format, are informed of their responsibilities.

e. County of Sacramento workforce members who fail to comply with County of Sacramento HIPAA policies and procedures to safeguard clients' PHI are subject to sanctions.

f. County of Sacramento workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's PHI are subject to criminal investigation and prosecution or civil monetary penalties.

g. Reported violations will be investigated and appropriate sanctions will be brought against workforce members who violate County of Sacramento HIPAA Policies and Procedures.

h. If County of Sacramento fails to enforce privacy safeguards and apply appropriate sanctions against workforce members who fail to comply with County of Sacramento HIPAA policies and procedures, County of Sacramento may be subject to administrative penalties by the United States Department of Health and Human Services (DHHS), including federal funding penalties.

2. Whistleblower retaliation prohibited

a. Neither County of Sacramento as an entity nor any County of Sacramento workforce member will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:

i. Any individual for exercising any right established under County of Sacramento policy, or for participating in any process established under County of Sacramento policy, including the filing of a complaint with County of Sacramento or with the United States Department of Health and Human Services Office for Civil Rights (OCR).

ii. Any individual or other person for:

A. Filing of a complaint with County of Sacramento or with OCR as provided in County of Sacramento HIPAA Privacy Rule policies;

B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to County of Sacramento HIPAA policies;

C. Opposing any unlawful act or practice, provided that:

I. The individual or other person (including a County of Sacramento workforce member) has a good faith belief that the act or practice being opposed is unlawful; and

II. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's PHI in violation of County of Sacramento policy.

3. Disclosures by whistleblowers and workforce crime victims

a. A County of Sacramento workforce member or business associate may disclose a client's PHI if:

i. The County of Sacramento workforce member or business associate believes, in good faith, that County of Sacramento has engaged in conduct that is unlawful or that otherwise violates professional standards or County of Sacramento policy, or that the care, services, or conditions provided by County of Sacramento could endanger County of Sacramento staff, persons in County of Sacramento care, or the public; **and**

ii. The disclosure is to:

A. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of County of Sacramento;

B. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by County of Sacramento; or

C. An attorney retained by or on behalf of the County of Sacramento workforce member or business associate for the purpose of determining the legal options of the County of Sacramento workforce member or business associate with regard to this County of Sacramento policy.

b. A County of Sacramento workforce member may disclose limited PHI about an individual to a law enforcement official if the workforce member is the victim of a criminal act and the disclosure is:

i. About only the suspected perpetrator of the criminal act; and

ii. Limited to the following information about the suspected perpetrator:

A. Name and address;

B. Date and place of birth;

C. Social security number;

D. ABO blood type and Rh factor;

E. Type of any injury;

F. Date and time of any treatment; and

G. Date and time of death, if applicable.

Procedure:

1. General

a. County of Sacramento workforce members who violate County of Sacramento policies and procedures regarding the safeguarding of an individual's PHI are subject to:

i. Appropriate disciplinary action by County of Sacramento, up to and including immediate dismissal from employment.

ii. The type of disciplinary action shall be determined by the HIPAA-covered component.

iii. The HIPAA-covered component may consult with the Office of Personnel Services and/or County Counsel to determine the appropriate sanctions.

iv. Personnel sanctions shall be documented by the Office of Personnel Services.

b. County of Sacramento workforce members who knowing and willfully violate state or federal law for improper invasions of personal privacy may be subject to reporting to appropriate local, state or federal law enforcement or regulatory agencies:

   i. Criminal investigation and prosecution, both by the County of Sacramento and by the federal government, depending on the nature of the violation. Federal and state law provides substantial fines and prison sentences upon conviction, depending on the nature and severity of the violation.

   ii. Civil monetary penalties that the Federal Department of Health and Human Services (DHHS) may impose, as described in 45 CFR 160.404.

   iii. Workforce members may be individually liable for accreditation, licensure sanctions, or even criminal and civil prosecutions and penalties under other Federal or State regulations.

c. Improper uses and disclosures of PHI shall be reported as security incidents and investigated by the Office of Compliance.

   i. Refer to County of Sacramento HIPAA Security Rule Policies 9 and 16.

d. County of Sacramento shall mitigate, to the extent practicable, any harmful effect that is known to County of Sacramento of a use or disclosure of PHI in violation of its policies and procedures.

Form(s):

- County of Sacramento HIPAA Privacy & Security Policy and Procedures Acknowledgement Form 3013

Reference(s):

- 45 CFR Parts160.404-160.408 and Part164.530
- County of Sacramento HIPAA Security Rule Policies and Procedures, Policy 9: Security Incidents and Response
- County of Sacramento HIPAA Security Rule Policies and Procedures, Policy 16: Sanctions

Policy AS-100-10: Group Health Plans

Issue Date: April 14, 2003
Effective Date: April 14, 2003
Revised Date: January 2, 2018

NOTICE: Under the federal Health Insurance Portability And Accountability Act (HIPAA), those provisions of HIPAA concerning the privacy and confidentiality of a person's health confidential information "give way" to those California state law provisions, and other federal law provisions, that are more stringent than HIPAA.

County staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the Office of Compliance or County Counsel.

Purpose:

The HIPAA Privacy Rule identifies special requirements for Group Health Plans.
A Group Health Plan means an employee welfare benefit plan or program that provides or pays the cost of medical care, including insured and self-insured plans, maintained by an employer, that to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

a. Has 50 or more clients; or

b. Is administered by an entity other than the employer that established and maintains the plan.

Policy:

1. Requirements for Group Health Plans

a. A group health plan, in order to disclose protected health information (PHI) to the plan sponsor (a plan sponsor is an employer (i.e., the County of Sacramento) or to provide for or permit the disclosure of PHI to the plan sponsor by a health insurance issuer or health maintenance operation (HMO) with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this policy.

b. The group health plan, or a health insurance issuer or HMO with respect to the

group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of:

i. Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

ii. Modifying, amending, or terminating the group health plan.

c. The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

d. As plan sponsor, the County of Sacramento is required to appropriately safeguard PHI created, received, maintained or transferred to or by the plan sponsor on behalf of the group health plan.

2. Notice of Privacy Practices

a. An individual enrolled in a group health plan has a right to notice:

i. From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

ii. From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

b. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives health information in addition to summary health information or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

i. Maintain a notice under this section; and

ii. Provide such notice upon request to any person.

c. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive health information other than summary health information or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice.

d. Other Notice of Privacy Practices Requirements for Health Plans

i. The County of Sacramento health plans must provide a Notice of Privacy Practices:

A. No later than the compliance date for the health plan, to individuals then covered by the plan;

B. Thereafter, at the time of enrollment, to clients who are new enrollees; and

C. Must notify clients then covered by the plan no less frequently than once every three years of the availability of the Notice and how to obtain the Notice.

D. If there is a material change, the Group health plan must:

I. Prominently post the change or its revised Notice on its website by the effective date of the material change; and

II. Provide the revised Notice, or information about the material change and how to obtain the revised Notice, in the next annual mailing to the individuals then covered by the plan.

III. In the event the group health plan does not post its Notice, the group health plan must provide the revised Notice, or information about the material change and how to obtain the revised Notice, to clients then covered by the plan within 60 days of the material revision to the Notice.

E. The County shall prominently post the Notice of Privacy Practices on the Office of Compliance internet web site and make the notice available electronically through the web site. The website is: http://www.compliance.saccounty.net.

Procedure:

1. Requirements for Group Health Plan Documents

a. The plan documents of the group health plan must be amended (only if health information other than summary health information is sought) to incorporate provisions to:

i. Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

ii. Provide that the group health plan will disclose PHI to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

A. Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

B. Ensure that any agents, including a subcontractor, to whom it provides PHI received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

C. Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

D. Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

E. Make available PHI in accordance to individuals' right to access their health information;

F. Make available health information for amendment and incorporate any amendments to health information;

G. Make available the information required to provide an accounting of disclosures;

H. Make its internal practices, books, and records relating to the use and disclosure of health information received from the group health plan available to the federal Department of Health and Human Services Secretary for purposes of determining compliance;

I. If feasible, return or destroy all PHI received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

b. Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

i. Describe those employees or classes of employees or other persons under

the control of the plan sponsor to be given access to the health information to be disclosed, provided that any employee or person who receives health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

ii. Restrict the access to and use by such employees and other persons to the plan administration functions that the plan sponsor performs for the group health plan; and

iii. Provide an effective mechanism for resolving any issues of noncompliance by persons with the plan document.

2. Uses and Disclosures

A group health plan may use and disclose PHI as follows, only to the extent that the group health plan has been amended consistent with Policy 1, above:

a. May disclose health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs.

b. May not permit a health insurance issuer or HMO with respect to the group health plan to disclose health information to the plan sponsor except as permitted by this policy.

c. Not disclose and may not permit a health insurance issuer or HMO to disclose PHI to a plan sponsor as otherwise permitted this policy and is included in the appropriate notice; and

d. Not disclose PHI to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

e. Health plans, including group health plans, health insurance issuers (including HMOs) and issuers of Medicare supplemental policies, are prohibited from using or disclosing genetic information for underwriting purposes.

f. A group health plan shall ensure that any agents to whom it provides PHI received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information.

3. Provision of Notice

a. Requirements for County of Sacramento health plans only.

i. The County of Sacramento health plans must provide a Notice of Privacy Practices:

A. No later than the compliance date for the health plan, to individuals then covered by the plan;

A. Thereafter, at the time of enrollment, to clients who are new enrollees; and

B. Must notify clients then covered by the plan no less frequently than once every three years of the availability of the Notice and how to obtain the Notice.

I. The Office of Compliance will coordinate this notification with County of Sacramento Health Plans

II. To the named insured of the health plan policy.

C. If there is a material change, the County's health plans must:

I. Prominently post the change or its revised Notice on their websites by the effective date of the material change; and

II. Provide the revised Notice, or information about the material change and how to obtain the revised Notice, in their next annual mailing to the individuals then covered by the plan.

III. In the event the health plan does not post its notice, the health plan must provide the revised Notice, or information about the material change and how to obtain the revised Notice, to clients then covered by the plan within 60 days of the material revision to the Notice.

A) The County shall prominently post the notice of privacy practices on the Office of Compliance internet web site and make the notice available electronically through the web site. The website is: http://www.compliance.saccounty.net.

B) The County's Personnel Services' Benefits office shall also post the Notice of Privacy Practices on its website: http://inside.personnelservices.saccounty.net/Benefits/Documents (listed as "Privacy Notice").

Reference(s):

- 45 CFR Part 164.314, Part 164.504 and Part164.520

Form(s):

- Notice of Privacy Practices