County of Sacramento — Office of Compliance

HIPAA PRIVACY & SECURITY RULE TRAINING
TEMPORARY AGENCY, VOLUNTEERS, REGISTRY & CONTRACTORS
Health Insurance Portability and Accountability Act (HIPAA)

Your Role	You are responsible for protecting the confidential information of the County's clients by complying with the County's HIPAA Policies and Procedures. 1. Read this training to learn how to comply. 2. Sign the Acknowledgment Form on the last page. **Contact your supervisor at the County if you are unsure how to comply.**
What is HIPAA?	HIPAA is a federal law that: • Requires the protection and confidential handling of Protected Health Information • Mandates industry-wide standards for health care information on electronic billing and other processes • Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs • Reduces health care fraud and abuse
County Privacy Rule and Security Rule Policies and Procedures	The County's HIPAA Policies and Procedures address the Privacy Rule and Security Rule requirements in the HIPAA Administration Simplification Rule 45 Code of Federal Regulations (CFR) Part 160, General Administration; and Part 164, Privacy and Security Rules. • The HIPAA Privacy Rule provides federal protections for Protected Health Information (PHI) and gives patients an array of rights with respect to that information. • The Security Rule specifies a series of administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of Protected Health Information (PHI), especially electronic PHI also known as Electronic Health Records (EHR). The Policies and Procedures are available at: Internet: https://insidecompliance.saccounty.gov/Pages/default.aspx Intranet: https://compliance.saccounty.gov/Pages/default.aspx
How Does HIPAA Work With State Laws?	HIPAA creates a federal privacy floor (minimum requirement) and supersedes any contrary state law. Note: State law governs if it is more stringent than HIPAA, providing greater privacy protections.

Client Rights	HIPAA guarantees certain rights to clients including: • Right to receive a Notice of Privacy Practices (NOPPs). You will be trained at your work site in the specific procedures used by your program. • Right to access, inspect, and receive a copy of their own PHI with exception of psychotherapy notes or information compiled for legal proceeding. • Right to request and receive an accounting of disclosures of their PHI. • Right to request to amend or correct their records if they are incorrect. • Right to request additional protections such as confidential communication, receiving PHI at alternate locations, or by alternative means. • Right to request restrictions of use or disclosure of PHI. Immediately refer client requests for any restrictions to your supervisor for action. • Right to file a Privacy Complaint. • Right to receive notification if their PHI is breached.
HIPAA Applicability The HIPAA Privacy and Security Rules Apply Only to Covered Entities (and Business Associates)	The County of Sacramento's HIPAA-covered components include: • Health care providers who electronically transmit health information Examples: Physicians, hospitals, labs, public health departments (Excludes providers who submit transactions on paper.) • Health plans who provide or pay the cost of medical care Examples: Medicaid, Medicare, Blue Cross • Business Associates (BAs) and their subcontractors Examples: Interpreters, Registry & Temporary Employee Agencies, Electronic Medical Record vendors, Records Storage, After-hours Medical Advice Providers, Confidential Shred/Destruction companies • Programs and workforce members who support health care providers or health plans A list of the covered components is on the Compliance website: https://insidecompliance.saccounty.gov/Pages/default.aspx **Individuals such as you who are assigned to work in a HIPAA-covered program must comply with HIPAA regulations to protect the confidentiality and security of PHI.**

What Does HIPAA address?	• When and how a covered entity or BA may use or disclose Protected Health Information and electronic Protected Health Information (**PHI and ePHI**). • Sets boundaries on the use and disclosure of health records. • Individuals' rights with respect to their PHI and ePHI - gives clients more control over their health information. • Organizational requirements – what the County of Sacramento is required to do - establishes safeguards to protect privacy of health information. • Relationships between HIPAA covered entities and those not covered by HIPAA. • Civil and criminal penalties for HIPAA violations.
What is "Covered Information" According to HIPAA?	**All** Protected Health Information (PHI) held or disclosed by a covered entity or BA in **any** form, whether in paper records, communicated orally, on computers or in other electronic format. PHI is found, for example, in medical records, billing records, insurance/benefit enrollment, case or medical management records, prescription fulfillment systems, etc.
What is Protected Health Information–PHI (and ePHI)?	**PHI** is health information in any form or medium that identifies an individual, and relates to: • The individual's past, present, or future physical or mental health 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. **Electronic Protected Health Information (ePHI)** refers to health information that a HIPAA covered entity creates or receives in electronic (computer) media and/or is maintained in any form of electronic media, including but not limited to: • Computer files, email, electronic medical records • Shared network drives for HIPAA covered programs. • Laptop computers, CDs, USB drives, smartphones, tablets, or any portable electronic device.

PHI is Medical Information That is Personally Identifiable	Identifiers include the following: Names, street addresses - city, county precinct, zip codes (all geographic subdivisions smaller than a state... All elements of dates (except year) including birth date, admission date, discharge date, date of death... Telephone numbers, fax numbers, Social Security numbers, medical records numbers, health plan beneficiary numbers, account numbers, vehicle identifiers and serial numbers, including license plate numbers, health plan beneficiary numbers… Email addresses, web site addresses (URLs), internet protocol (IP) addresses… Biometric identifiers, including finger and voice prints and full-face photographic images or any comparable images of an individual, DNA/genetic information.
PHI Does Not Include	• Education records, Workman's Compensation records or health information in your employment records. These records are not covered by HIPAA because they do not belong to HIPAA covered entities. However, this information is protected under other laws. • Records held by non-HIPAA entities such as Children's Protective Services, Adult Protective Services, WIC, and government-funded programs whose primary mission is not providing for or paying the cost of medical care.
HIPAA Security Awareness – What is it?	• Recognizing what types of security issues may arise in the workplace; and • Knowing what actions to take in the event of a security breach.

Always Report Incidents involving PHI
 	
Notify Your Supervisor If You Suspect A Security Incident Or Contact The Office Of Compliance at 874-2999 / HIPAAOffice@saccounty.gov
	Examples of potential security incidents:
	• Suspected or actual unauthorized viewing of PHI or EPHI--including fax or email sent to incorrect recipient.
	• Unencrypted email that contains PHI.
	• Lost, stolen or missing PHI due to disaster, failure, error, or theft.
	• Lost, stolen or missing electronic media or device (computer, laptop, iPhone or iPad, other smartphone, CD, USB drive, etc.) that contains EPHI.
	• Loss of the integrity (alteration or corruption) of PHI or EPHI.
	• Virus, worm, or other malicious code attacks.
	• Persistent network or system intrusion attempts from a particular entity.
	• Unauthorized access to PHI, EPHI, or an EPHI based system or network.
	• Unauthorized verbal disclosure.
	• Facility incidents (also contact the Facility Manager), including but not limited to:
	  ○ Unauthorized individual found in a HIPAA covered component's secured area where PHI or EPHI is held.
	  ○ Facility break-in, broken doors, locks or windows.
	  ○ Lost, missing or stolen key, C-Cure badge or cardkey.

Safeguards You Must Follow	The County has Administrative, Technical and Physical Safeguards to protect PHI. Use available safeguards to keep all PHI private and secure.
Facility Safeguards	Protect confidential information, equipment and County buildings from unauthorized access. • **Always** immediately report missing, lost or stolen cards, metal keys or keypad-cipher lock combinations. • **Always** wear and display your County ID badge in the workplace to identify that you're authorized. • **Always** report any suspicious activities or unknown people in your facility. • **Always** report ASAP missing, lost or stolen access cards, badges, or keys • **Always** report any broken locks, doors or windows. • **Never** share access cards, keys or codes to enter our facility. • **Never** allow another employee to enter the facility behind you unless that individual has used a valid access card. Tailgating is not allowed.

Workplace Safeguards	It's your responsibility to make sure that PHI is not accessible or viewable by anyone except those who need it to do their job. • **Always** lock your computer any time you leave it unattended, even if it is only for a few minutes. • **Always** put away paper PHI any time you leave it unattended, even if it is only for a few minutes. • **Always** secure PHI in locked file cabinets after hours. • **Always** close doors or draw privacy curtains/screens for privacy. • **Always** return medical records to appropriate, secure location where unauthorized individuals cannot see them or access them. • **Always** make sure copies of PHI at copy machines, printers, or fax machines are retrieved immediately. • **Always** check hard copy mail to make sure you are sending to the correct recipient(s). • **Always** dispose of paper containing PHI properly in a locked shred bin. • **Never** share PHI with unauthorized individuals or have it viewable in public areas. • **Never** leave PHI exposed in mail boxes or conference rooms. • **Never** put any PHI into garbage or recycling containers.
Workstation Protection	Properly safeguarding each workplace computer is one of the most important ways to protect your program's data from corruption or loss. • **Log off** when you are done working on your computer. • **Lock your computer** session when it is left unattended (See below for instructions). • **Protect ePHI from unauthorized access** if you work from home or other non-office work sites on a County assignment. • **Report** viruses or unusual computer behavior to the Service Desk at 916-874-5555.
How to lock your computer session	Prevent unauthorized viewing or access of PHI on your computer. County HIPAA Policies and Procedures require that you manually lock your computer session every time you leave it. 1. Hold down the Ctrl + Alt + Delete keys on your computer then press "Enter" key. 2. Using your mouse, click "LOCK COMPUTER" **–or–** Simply press the Windows and L keys to lock your computer 3. To unlock your computer session hold down the Ctrl + Alt + Delete keys on your computer (or enter Windows and L keys) 4. Type in your password and press enter Locking your computer session when you leave your computer unattended does not shut down any document or program you have been working on.

Computer Safeguards	• **Always** store all data on network servers (not on the C:\ drive). • **Always** lock your computer session when left unattended. • **Always** report any suspected security violation. • **Always** lock ePHI at remote sites. • **Always** know who to contact for your questions. • **Never** share a log-on ID or password. • **Never** write down or share your password. • **Always** report issues to the Service Desk (916-874-5555).
Internet Safeguards	• **Always** be cautious when visiting unfamiliar websites and avoid them when possible. • **Never** open an attachment in an email you were not expecting. • **Never** click on links in unsolicited emails. • **Never** click on popup windows. • **Never** change the Internet security settings on your County computer. • **Never** download unapproved software, files, music, games, video downloads, or screensavers. • **Never** use USB drives that were not provided by the County. • **Never** access PHI from locations with public Wi-Fi. • **Always call the Service Desk about any suspected virus!!**
Select A Secure and Strong Password	**What is a STRONG password?** A strong password has a *minimum* of eight characters and should contain *at least one of each* of the following characters: • Uppercase letters (A-Z) • Lowercase letters (a-z) • Numbers (0-9) • Punctuation marks or symbols such as: !@#$%^&*()_+=- **How to create a strong and secure password:** 1. **Create a password from a sentence you can remember, like "My son John is two years old today"** Use first letters to form the password: msjityot 2. **Add complexity with upper case letters and numbers (and special characters)** MsJi2Y0t M$JI2y@t 3. **Don't use your work password on Internet** Website security could be compromised Keystroke logging devices may be on public computers

The Rules for Secure Password Management	• You will be required to change your password every 6 months. • **Never** tell or share your password with anyone. • Do not write down your password. • Create a password that's hard to guess. • Do not use a word from the dictionary or anything thing that can be associated with you (such as birth or anniversary dates). • **Never** share your user ID or password with anyone. • If you think someone has learned your password, change it immediately.
.Secure Faxing and Email	• **Always** obtain the supervisor's approval before sending PHI in email. • **Always** encrypt ALL email containing PHI that is sent outside the County network (@saccounty.gov). • **Always** check the email thread to see if you really need to send all of it. It's okay to start a new email. • **Always** check recipients are correct before sending faxes or email to make sure you are sending them to the intended, authorized recipient(s). • **Always** check content and attachments in faxes and emails before sending to verify that you are sending what you intend to send. • **Always** make sure the intended recipient(s) received your email or fax. • **Always** use a cover sheet with a privacy statement and clear instructions on how to reach you in the event the wrong individual receives the fax. • **Never** "reply all" or forward emails that have too much information unless ALL recipients need all the information. Use the minimum necessary standard. • **Never** put PHI in the Subject line of an email or on the fax cover sheet.
Hard copy mail	• **Always** check the name and address are correct before mailing. • **Always** make sure the addressee on the document is the same as the addressee on the envelope. • **If possible,** use a cover sheet with a privacy statement and clear instructions on how to reach you in the event the wrong individual receives the mail.
Verbal Safeguards	• **Always** be aware of your surroundings and of anyone who might overhear PHI. • **Always** ensure privacy when speaking about confidential matters (both PHI and PII), and use the minimum necessary standard. • **Always** keep space between clients when they're checking in. • **Never** share information you have learned while performing your job with any County employee who does not need to know it to do their job, or with anyone outside of the workplace, including family members or friends.

Other safeguards	• **Always** obtain the supervisor's approval before downloading data. • **Always** secure mobile devices that contain ePHI with passwords and encryption and keep the device with you at all times. • **Always** make sure that any PHI or ePHI that is taken off site is attended and supervised at all times, and stored in a secure manner.
The Difference Between "Use" and "Disclosure" of PHI	• **USE** - The ***sharing***, employment, application, utilization, examination, or analysis of Protected Health Information (PHI) ***within*** (**inside**) the entity that maintains the PHI. • **DISCLOSURE** - The ***release***, transfer, provision of access to, or divulging in any other manner of PHI ***outside*** the entity holding the information.
HIPAA Rules About Use and Disclosure of PHI	The County of Sacramento workforce members may only use or disclose PHI for *purposes permitted or required* and in *ways that are permitted or required* by HIPAA. A use or disclosure that is not permitted or required by the rule is prohibited by the law. In most cases, use or disclosure must comply with the Minimum Necessary Standard.
Minimum Necessary Standard	The "MINIMUM NECESSARY" and "NEED TO KNOW" standards should apply in all your access of PHI and ePHI. Ask yourself these questions: • Is it necessary for your job? • How much do you need to know? • How much do other people need to know? The HIPAA Privacy Rule states that a covered component may provide only the minimum necessary amount of PHI necessary: • To accomplish the purpose for which use or disclosure is sought. • To those among the workforce who need the information to perform their job.
Exceptions to the Minimum Necessary Standard	The Minimum Necessary standard does not apply to: • Disclosure to or request by a health care provider for treatment purposes. (*However, the minimum necessary standard does apply to 'P' (payment) and 'O' (operations) of TPO*.) • Disclosures to the client who is the subject of information. (*However, access to the client can be limited under certain conditions*.) • Uses or disclosures authorized by client. (*However, only what is authorized may be disclosed.*) • Uses or disclosures required by law. • Disclosures to U.S. DHHS for compliance/enforcement activities. • Uses or disclosures required for compliance with standard transactions (in connection with billing, etc.).

Always Verify Identity Before Disclosing PHI	• Always verify the identity of the individual requesting the information and their authority to have access to the PHI. • Make sure you're disclosing the correct individual's information. • Check for disclosure restrictions.
County's Requirements for Verifying Identity	• Verify identity with a **photo ID** such as a driver's license or state ID card **or two or more of the following**: military ID, military discharge papers, government employee badge, naturalization papers, immigration cards, certified copy of birth certificate, passport, check cashing card, food stamp ID card. • Verify by asking the individual their first and last name and other personal identifiers (such as birth date, address, last four numbers of social security number, etc.). Always refer the request for release and verifying documents immediately to your supervisor.
What is a "Personal Representative"?	A "personal representative" is an individual with authority to act on behalf of an individual in making decisions related to health care. General rule: treat a personal representative as if they were the individual. Limitation: the individual is treated as a personal representative only with respect to PHI that is relevant to the personal representation. If the parent's last name is different from child's last name, determine relationship to child. *Before releasing health information about a minor child under the care of a guardian (or other individual acting in place of the parent), request copies of guardianship papers and refer the request for disclosure to your supervisor for determination.*
What Are Required Disclosures?	HIPAA requires disclosure of PHI: • Upon request by the individual who is the subject of the information. • When the Office for Civil Rights, under the direction of the Federal U.S. DHHS, investigates compliance or violations of privacy and security. • As required by law.
What Are Permitted Uses and Disclosures?	• Uses and disclosures for treatment, payment, and health care operations (TPO). • Uses and disclosures that require the individual's permission. • Those requiring an authorization from the individual. • Those where the individual must be given an opportunity to agree or object. • Certain limited uses and disclosures for important governmental purposes. ***Contact your supervisor if you are unsure whether you may use or disclose PHI.***

Uses and Disclosures for Treatment, Payment and Operations (TPO)	Under HIPAA, client written authorization is not required, and a covered entity may use and disclose PHI: • For its own TPO. • For treatment activities of any health care provider. • For payment activities of any health care provider. • For health care operations of another covered entity (under some circumstances). Definition of Treatment: *Providing*, coordinating or managing health care; *coordinating* and *managing* health care by a health care provider with a third party; *consultations* among health care providers; *referrals* of patients from one health care provider to another. Definition of Payment: Obtaining premiums (not applicable to Medicaid) or fulfilling obligations for coverage and the provision of benefits (*example*: Medicaid eligibility); obtaining or providing reimbursement (*example*: Medicaid payment of claims). A HIPAA covered entity may release PHI for payment purposes to non-covered organizations or components within its own organization (*example*: PHI may be disclosed to obtain reimbursement from a disability insurance carrier). Definition of Health Care Operations: Administrative and business management activities of the covered entity. Some of these include: quality assessment; development of clinical guidelines; case management and care coordination; sharing information about treatment alternatives; competency and performance reviews; training programs; fraud and abuse detection, patient safety activities and compliance programs.
What Types of Uses or Disclosures *Always* Require An Authorization?	Authorizations are required for disclosures of PHI for purposes other than TPO: 1. That are not otherwise allowed under the Privacy Rule 2. For disclosures to third parties specified by the client 3. To use or disclose psychotherapy notes Authorizations may be initiated by the client or by the County of Sacramento (*examples*: Client wants PHI disclosed for life insurance application; client wants their PHI sent to their attorney; health care worker wants to help client apply for disability benefits).

What Does a County Authorization Form (also known as Release of Information) Need to Include to be Valid?	When you fill out the County's HIPAA Form 2099 – "Authorization to Obtain and/or Release Medical Records" – the Form 2099 MUST include the following: • A description of information to be used or disclosed that identifies the information in a specific, meaningful fashion (I: Discharge summary, laboratory reports, clinical reports, etc.). • The name (specific identification) of the individual(s) authorized to request the use or disclosure. • The name (specific identification) of the individual(s) to whom the covered health care component is making the requested use or disclosure (examples: Law firm of Smith and Jones, Johnson Corporation – Diabetes Research Project staff, etc.). • The expiration date that relates to the client and purpose for use or disclosure (examples: 90 days from date authorization is signed; 30 days post discharge, etc.). County policy requires it must be no longer than one year. • Description of each purpose of requested use or disclosure. • If authorization is client-initiated, it is sufficient to state "At the request of the individual." • Signature of client or personal representative and date of the authorization. • Description of personal representative's authority to sign for client (*example*: guardian of individual). • Advise patients they can refuse to sign. The County may not condition treatment, payment, and/or enrollment in a health plan or eligibility for benefits on signing of authorization by client *except*, A.) If the County is providing health care solely for the purpose of creating PHI for disclosure to third party (*example*: life insurance physical) or B) prior to enrollment in a health plan if authorization is for eligibility or enrollment determinations.
When is an Authorization Form Invalid?	• When the expiration date has passed, or the expiration event is known to have occurred. • When it is not filled out completely with all required elements listed above. • When it is revoked by client. • When information in the authorization is known by component to be false. • When the authorization is combined with any other document.

Can PHI be Disclosed to Family Members or Friends?	Yes, under certain circumstances, such as: • Use or disclosure of PHI to notify or assist in notification of individual's location, or general condition is permitted if the individual is first given opportunity to agree or object. Verbal agreement is possible if the client is given the opportunity to object to the disclosure and does not object or if you, as a health care provider, can reasonably conclude the client agrees (*example*: the client asks a friend to remain during the medical exam). • If a client is not able to respond (*examples*: incapacitated, in an emergency situation or dead) *or* if the client is not present, the health care provider may use or disclose PHI directly relevant to the individual's involvement if, based upon professional judgment, disclosure is in the best interest of the client (*example*: a designated relative is picking up a prescription) **Note: Check for restrictions before sharing PHI with the client's family members or friends!**
Situations That Do Not Require an Authorization to Use or Disclose	Covered health care components may use or disclose PHI without an authorization under the following exceptions. **In every situation, do not release any information, and refer the request for use or disclosure to your supervisor.** • **Activities involving Public Health** – No authorization is needed to release PHI to public health authorities who, by law, collect or receive PHI to prevent or control disease, injury, disability, or for public health surveillance, investigations, or interventions. Do not take action on any request for release of PHI to public health authorities without consulting your supervisor. There are specific procedures in each of the County's covered components for responding to these requests. • **Child Abuse or Neglect** - To a government authority (*example*: Child Protective Services – CPS) authorized by law to receive reports of child abuse or neglect. Child abuse reporting is considered a "Public Health Activity". Do not take action on any report of child abuse or neglect. Immediately refer the matter to your supervisor for evaluation under state and federal laws as well as County policies and procedures. • **Adult abuse, neglect, or domestic violence** – HIPAA covered health care components may disclose the victim's PHI in order to report abuse, neglect, or domestic violence (when required by law and necessary to prevent serious harm). Do not take action on any report of adult abuse, neglect or domestic violence without consulting your supervisor. **(continued on next page)**

Other Situations That Do Not Require an Authorization to Use or Disclose **(continued)**	• **Health oversight activities –** PHI can be disclosed to public oversight agencies (and to private entities acting on behalf of public agencies) without client authorization for activities authorized by law such as: audits (example: Medicaid audits); civil, administrative or criminal investigations; inspections and disciplinary. Do not take action on any release of PHI to public oversight agencies. Refer any such request to your immediate supervisor. • **Judicial and administrative proceedings** – PHI may be released without authorization as required by law, such as State statutes and administrative codes; Federal law; court orders; court-ordered warrants; subpoenas, summons from a court, grand jury, discovery request or other lawful process. Do not take action on any request for release by a court order, subpoena, discovery request or other lawful process. Refer any such request to your immediate supervisor. There are specific procedures in each of the County's covered components for these legal/judicial requests. • **Some limited law enforcement purposes** – A covered health care component may disclose **limited** PHI to law enforcement officials (LEO) as required by law. Do not take action on any request for release of PHI by law enforcement officials. Refer any such request to your immediate supervisor. There are specific procedures in each of the County's covered components for these law enforcement requests for disclosure of PHI, including reporting. • **Decedents** – A covered health care component can disclose PHI to coroners and medical examiners for identification of a deceased individual, determining cause of death or other duties authorized by law. PHI can be disclosed to funeral directors when it is consistent with applicable law, to carry out their duties w/respect to the decedent, prior to and in reasonable anticipation of death (*example*: pre-pay burial arrangement). A covered health care component may also disclose PHI about the deceased to LEO when there is suspicion that death may have resulted from criminal conduct. Do not take action on any request for release of PHI by a coroner, medical examiner or funeral director. Refer any such request to your immediate supervisor. There are specific procedures in each of the County's covered components for these requests for disclosure of PHI. **(continued on next page)**

Other Situations That Do Not Require an Authorization to Use or Disclose (continued)	• **Serious threat to health or safety** – A covered health care component may, in good faith, use or disclose PHI when consistent with applicable law, and when, in good faith, it believes it is necessary to prevent or lessen serious and imminent threat to health or safety of an individual (or public). There are specific limitations to the information that can be released. Do not take action on any release of PHI where a potential threat to health or safety may be identified. Immediately refer the matter to your immediate supervisor for evaluation under state and federal laws as well as County policies and procedures. • **Other specialized government functions** – these include the following: Corrections and Lawful Custody. A covered health care component may disclose PHI to a correctional institution (prison, jail, reformatory, detention center, halfway house, residential community program center) or to LEO having lawful custody of inmate or other individual. An individual is no longer an inmate when released on parole, probation, supervised release, or no longer in lawful custody. Do not take action on any release of PHI regarding an individual in lawful custody. Refer the request to your supervisor for evaluation and direction. Government Programs providing Public Benefits. Covered health plans that are government programs providing public benefits may disclose PHI relating to eligibility or enrollment in the health plan to another agency administering a government program providing public benefits under certain conditions. Do not take action on any release of PHI in connection with providing public benefits. Refer the request to your supervisor for evaluation and direction. • **Workers' Compensation** - Covered components may disclose PHI in accordance with workers' compensation. Workers' compensation programs are not covered under HIPAA. • **Employers – Public Health Activities** - No authorization is required to release PHI to an employer about a member of the workforce under certain conditions. The healthcare provider (County of Sacramento) must give written notice that PHI related to work-related illness, injury, or surveillance is disclosed to the employer. Do not take action on any request for release of PHI from an employer regarding a member of their workforce. Refer this immediately to your supervisor.

Is the County Required to Track Disclosures of PHI and ePHI?	Yes, under HIPAA, covered health care components are required to track certain disclosures of PHI and there is a specific HIPAA form to use (County Form 2097, "Accounting of Disclosures" or equivalent form created by the EHR). Electronic Medical Records (EMRs) will use a format similar to the Accounting of Disclosures form that contains the information required by the Accounting of Disclosures. A client has a right to receive a written accounting of those disclosures of their PHI in the six years prior to the date on which the accounting was requested,. **Your supervisor will train you how to use the disclosure form at your work site, along with specific procedures from the department, division or program where you are placed.**
Information Required in the Accounting of Disclosures	The following content is required to be included in an Accounting of Disclosure: • Date of disclosure. • Name (and address, if known) of entity or individual who received the PHI. • Brief description of the PHI disclosed. • Brief statement of disclosure's purpose. • Copy of written request for disclosure. Multiple disclosures to same entity/individual have specific content requirements. **Refer any circumstance of multiple disclosures of this type to your immediate supervisor for guidance in correct documentation.**
Types of Disclosures Tracked in the Accounting of Disclosures (Form 2097)	The disclosures which must be included are those for: • Disclosure for judicial and administrative proceedings, including a response to a subpoena or a court order. • Disclosure for public health activities, such as mandatory communicable disease reporting. • Disclosures to the FDA (e.g. medical device malfunctions, adverse events, vaccine reactions, etc.). • To report injuries by firearms, assaultive or abusive conduct. • Disclosure for adult or child abuse reporting purposes. • Disclosure (unless for TPO) to health oversight agencies for audits, civil or criminal investigations, inspections, licensure or disciplinary actions Disclosure to law enforcement in emergencies when a crime is suspected. • Disclosure to law enforcement for identification of a suspect or fugitive, or for locating a suspect or fugitive. • Disclosure about decedents to medical examiners, funeral directors, or coroners. • For cadaveric organ, eye or tissue donation. • Birth and death reporting. • Disclosure for a Worker's Compensation claim.

Disclosures of PHI NOT Required on the Accounting of Disclosures (Form 2097)	Not all disclosures require tracking. *Exceptions* are disclosures for: • Disclosures made for treatment, payment, or healthcare operations (TPO). • Disclosures authorized by the client or made to the client such as a copy of their medical record. • Disclosures made to a person authorized to be involved in the client's health care (personal representative). • Disclosures for use in a hospital directory. • Disclosures for national security or intelligence purposes to an authorized public official. • Disclosures made to correctional institutions or law enforcement officials having lawful custody of an inmate. • Incidental disclosures to a use or disclosure otherwise permitted or required by law.
Reproductive Health Care	Prohibition on use or disclosure only applies if the reproductive health care is: • Lawful under the law of the state where the care is provided and under the circumstances in which it is provided, or • It is protected, required or authorized by Federal law under the circumstances in which it is provided, regardless of the state where it is provided (e.g., Constitutional right to contraception, and emergency care required by EMTALA). There is an attestation requirement before the disclosure of reproductive health records in four situations. • Uses and disclosures for health oversight activities. • Disclosures for judicial and administrative proceedings. • Disclosures for law enforcement purposes. • Uses and Disclosures about decedents to Coroners and Medical Examiners. County workforce members must: • Carefully review requested records to see if they contain Protected Health Information potentially related to reproductive health care. • If they do, an attestation is required and there should be no response from anyone without assistance from County Counsel. • A completed attestation should be reviewed by County Counsel to verify that it is valid. • Information may they be sent in response to request.
Whistleblowers	HIPAA regulations permit workforce members to disclose PHI in order to expose unlawful or unprofessional conduct. Covered entities may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals who expose problems or bring complaints.

Sanctions: The Consequences of Violating HIPAA

Covered health care entities are required to develop a system of sanctions for employees who violate the entity's HIPAA policies. Sanctions for non-employees may include termination of employment and/or reporting to government agencies. These sanctions are not applicable to: whistleblowers (a member of the workforce who discloses information about a covered health care component); a member of the workforce who is a crime victim; or a workforce member filing a complaint with the Office for Civil Rights (OCR), testifying, assisting or participating in an investigation, compliance review or similar proceeding.

Examples of HIPAA Violations:

- Any negligent or intentional violation of the County HIPAA Policies and Procedures may result in such corrective action as deemed appropriate by the County.
- Any unauthorized, willful or malicious release of any information associated with PHI may result in personal civil or criminal liability.

Violations may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations.

There are both civil and criminal penalties that may be imposed by the OCR if their investigation determines a violation has taken place. Penalties for failure to comply with HIPAA are severe.

How is HIPAA Enforced?

The Federal Department of Health and Human Services has assigned enforcement activities to the Office for Civil Rights (OCR). Any individual or organization who believes a covered entity is not complying with HIPAA requirements may file a complaint with either the covered entity and/or the OCR. Complaints can be accepted only for possible violations occurring after the compliance date of April 14, 2003.

Penalty Tier	Level of Culpability	Minimum & Maximum Penalty per Violation (Updated August 2024)	Annual Penalty Limit
Tier 1	Reasonable Efforts Unaware of the HIPAA violation and by exercising reasonable due diligence would not have known HIPAA Rules had been violated.	$141 - $71,162	$2,134,831
Tier 2	Lack of Oversight Reasonable cause that the covered entity knew about or should have known about the violation by exercising reasonable due diligence.	$1,424 - $71,162	$2,134,831
Tier 3	Neglect – Rectified within 30 days Willful neglect of HIPAA Rules with the violation corrected within 30 days of discovery.	$14,232 - $71,162	$2,134,831
Tier 4	Neglect – Not Rectified within 30 days Willful neglect of HIPAA Rules and no effort made to correct the violation within 30 days of discovery.	$71,162 - $2,134,831	$2,134,831

HIPAA Administrative Requirements for the County	• Designate a County Privacy Officer and an Information Security Officer. • Provide workforce training on our HIPAA policies and procedures. • Administrative, Technical and Physical Safeguards. • Complaint process. • Appropriate workforce sanctions. • Mitigate to the extent feasible, any harmful effect resulting from a breach. • Refrain from intimidating acts against whistleblowers. • Provide services without requiring individuals to waive their privacy rights. • Written policies and procedures to protect PHI. • Document and maintain HIPAA-related information.
Role of the Office of Compliance	The Office of Compliance oversees the County's compliance with HIPAA and includes the following: Privacy and Security Training to HIPAA-covered programs; subject matter guidance to HIPAA-covered programs and workforce members; risk assessment and risk management; investigation of privacy complaints and security incidents relating to County clients' medical information; documentation of incidents and breaches and reporting of breaches to state and federal agencies; maintenance of HIPAA-related forms including release of information and other clients' rights forms. For more information, please contact: **County of Sacramento Office of Compliance** Phone: 916-874-2999 | Fax: 916-854-9507 Email: HIPAAOffice@saccounty.gov Intranet: https://insidecompliance.saccounty.gov/Pages/default.aspx Internet: https://compliance.saccounty.gov/Pages/default.aspx

Please see the Training Acknowledgment Form on the next page.

HIPAA Privacy & Security Rule Policies & Procedures Acknowledgment Form for Volunteers, County Contractors, and Temporary Agency or Registry Employees

Check one: ☐ Volunteer ☐ Contractor ☐ Temporary Agency employee ☐ Registry employee

I understand and agree to the following:

1. I am responsible for reviewing, understanding, and complying with the Countywide HIPAA Privacy & Security policies and procedures;
2. I will perform my duties in good faith and in a manner that is in the best interests of the County and the public it serves;
3. I will preserve client confidentiality, except as otherwise permitted or required by law, unless there is written permission to disclose information;
4. I will promptly report any activity that I believe in good faith may violate County HIPAA Privacy or Security policies and procedures, or any other applicable law, regulation, rule, or guideline, in accordance with the reporting procedures set forth in the County HIPAA policies and departmental policies and procedures;
5. I will comply with County HIPAA Privacy & Security Rule policies and procedures. When in doubt about what constitutes compliance performance, I will consult with my supervisor.

AFFIRMATION:

I certify that I have received training on the Sacramento County ("County") HIPAA Privacy and Security Policies and Procedures, and will comply with the County's HIPAA Privacy & Security Policies and Procedures.

If I violate either departmental or County HIPAA Privacy & Security Rule Policies and Procedures, I may lose any access privileges granted by the County or the department and be subject to disciplinary action up to and including termination. Willful or malicious release of any information associated with Protected Health Information may result in personal civil or criminal liability.

I understand that when necessary, I should seek advice from the appropriate supervisor concerning appropriate actions that I may need to take in order to comply with the HIPAA Privacy & Security Policies and Procedures.

NAME of Volunteer, Temp, Registry or Contractor (MUST PRINT)	***SIGNATURE***	***DATE***

County Department you're working for	***Name of your supervisor at the County***

Name of your Temporary Services or Registry Agency, or Employer (if Contracted) and contact information

DISTRIBUTION:

Distribute one copy to each:	**Distribute the original to (as applicable):**
☒ Individual who signed this form	☐ County Volunteer Coordinator
☒ Office of Compliance via Interoffice mail to MC 36-217. Questions? Call 874-2999.	☐ Your Contract Agency/Company
☐ Temps only: Department's Personnel Services Temp Coordinator	☐ Your Temporary Services Agency
☐ Temps only: County Personnel Services Temp Coordinator (Fax 874-4472)	☐ Your Registry Agency