MARIN HEALTH & HUMAN SERVICES
Health, Well-being & Safety

Benita McLarin, Director
Department of Health and Human Services

Confidentiality and Privacy in Health and Human Services

As employees and contractors of an agency that provides a range of health and social services to County of Marin residents, we are entrusted to protect the information with which we work. In your job, you may come into contact with client or consumer health information and other personal information, financial information, employee and payroll information and business information considered to be confidential by the County of Marin. Many of our programs are required to access or use information that is considered to be California State "Department PII". It is critically important that you protect any confidential information against disclosure to unauthorized individuals or entities. In addition to not disclosing confidential information, you must also take reasonable steps to ensure that the confidential information that you receive, regardless of its format, is protected from theft or unauthorized access. It is not only the law and our policy, it is a condition of employment and/or contract and detailed in the County Personnel Management Regulations (PMRs). Our collective effort to ensure the privacy and security of confidential information upholds the County's core values, demonstrates respect for our clients, and supports compliance with State and Federal laws. Your commitment to protecting our confidential information is an element of our success.

Note: While this document will focus primarily on Protected Health Information and Personally Identifiable Information, the principles will apply to all confidential information that you work with.

Brief Overview of Health Information Privacy and Security Regulations

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by the federal government to promote improvements and efficiencies in the provision of healthcare. A major goal of HIPAA was to protect the privacy and security of health information. HIPAA Regulations include the following parts:

- **Privacy:** The Privacy Rule provides the standards for the use and disclosure of Protected Health Information (PHI). It also gives individuals specific rights regarding their own health information.
- **Security:** The Security Rule governs how health information, in electronic format, is protected. They establish safeguards for Protected Health Information.
- **Breach Notification** : This Rule requires HIPAA covered entities and business associates to provide notice of a breach of unsecured PHI.

There are various other state and federal regulations that govern the privacy and security of health information and other personal information. Among the authorities that regulate our County work are: 42 CFR Part 2 (governing Substance Use Disorder patient records), Welfare and Institutions Code Section 5328-5830 (governing mental health client information) and Civil Codes Sections 1798.29, 1798.82 and 1798.84 (regulating the privacy of personal information), and the CA Confidentiality of Medical Information Act - Civil Code, Sections 56-56.37.

Protected Health Information (PHI) and Personally Identifiable Information (PII)

PHI is information related to an individual's physical or mental health condition, health care treatment and/or the corresponding payment for those services. PHI includes information that could reasonably identify an individual (client identifiers) and is connected to their health information. PHI in electronic, paper or oral forms must be protected. Every member of the workforce and certain independent contractors, even those who don't deal directly with client information, should have an understanding of what PHI is and the ways in which it must be protected.

- **Client identifiers:** Name, Street address, city, county, full zip code, dates directly related to an individual (e.g. birth date, dates of service), telephone and fax number, email address, social security number, credit card number, medical record or enrollment number, account number, certificate/license numbers, vehicle identifier, Internet Protocol (IP) address, biometric identifier (e.g. finger prints), full-face image, and any other unique identifying number, characteristic or code.
- **Health Information:** Diagnosis, Procedure or Procedure Codes, medication, physician name and specialty, location of service, (e.g. Cancer Center), service type (e.g. physician office, radiology, inpatient admission), test or lab results, amount(s) charged and paid.

Under California laws, PII that must be protected include:

- An individual's first name or first initial and last name, in combination with other data elements such as: social security number, driver's license number, account number, credit or debit card number, medical Information or health insurance information.
- User names or email addresses with the security code or password for accessing the online account.

"Department PII" is personally identifiable information directly obtained in the course of performing an administrative function through the MEDS or IEVS systems on behalf of the contracted state programs, which can be used alone, or in conjunction with any other reasonably available information to identify a specific individual.

Use of PHI/PII:

Employees and contractors in a healthcare or social services environment use PHI and/or PII daily to provide critical and routine services to our clients. Generally, PHI can be used and shared by a client's direct treatment team to provide healthcare services and for other operational purposes, such as billing. The permitted uses of PHI may differ slightly depending on the type of healthcare being provided in your division or program. Your supervisor will share more information about the appropriate uses of different types of confidential information. The HHS Confidentiality and Privacy Policy and Procedures can be found on the HHS Resources HUB and are incorporated by reference.

Minimum Necessary:

HIPAA requires that organizations take reasonable steps to allow access only to the minimum PHI necessary to perform a specific task or job. This minimum necessary standard applies to both internal uses as well as external disclosures. Employees, contractors and external providers must only receive information tailored to the specific task or job. It is important that you do not access, use or disclose more confidential information than you are authorized to access and that you need to complete your job. The minimum necessary standard is not intended to impede client care and therefore does not apply to qualified professionals involved in the direct care and treatment of the client.

Breach of PHI/PII:

Generally, there are "permitted" uses and disclosures of PHI/PII and "impermissible" uses or disclosures of PHI/PII. A breach is presumed when you use or disclosure PHI/PII in a manner not permitted by policy or law. A breach can be deliberate or accidental. Our goal as community partners, entrusted with confidential client and business information, is not to commit a breach of that confidential information. While our goal is to have no breaches, we understand that there may be times when a mistake is made and you access, use or disclose PHI, PII or other confidential information improperly. When or if this happens, it is our policy and the law that you immediately tell your supervisor and/or the Privacy Officer that you suspect there may have been a breach.

Disclosure of PHI/PII:

While you may access and use PHI/PII as part of your duties, you may also be asked to disclose PHI/PII to others for a variety of reasons. There are a few permitted reasons that you may disclose PHI/PII to others without a client's written permission or authorization. Healthcare providers may disclose PHI without a client's authorization for the purposes of treatment, payment or healthcare operations. The rules for disclosing PHI vary depending on the type of healthcare provider or the type treatment provided (for example Substance Use Disorder services are specifically protected by federal law), and you should familiarize yourself with all policies and regulations that apply to your area of work prior to disclosing any confidential information. If you are unsure about whether or not a disclosure may be permitted, ask your supervisor or the Privacy Officer for guidance prior to disclosing any information.

Authorization:

Generally, PHI may be used in a healthcare environment for treatment, payment or healthcare operations. A written authorization from the client is required for many uses and disclosures that fall outside of treatment, payment or healthcare operations. Health & Human Services has a form that a client may use, but occasionally another entity will present an authorization from the client requesting our records. It is important that no PHI/PII is disclosed unless the authorization form is determined to be valid and complete. Once an authorization is signed, a client has the right to revoke or cancel it at any time. HIPAA specifically states that care cannot be conditional upon a client's signing of an authorization. Until you are trained on the policies and procedures pertaining to disclosure of PHI or other confidential information in your area of work, you should request assistance from your supervisor.

Privacy and Security Policies and Procedures:

Be familiar with HIPAA privacy and security policies and procedures. The County of Marin and the Department of Health & Human Services has policies on privacy and security of personal and health information and they can be found on the HHS Resources Hub. You will be informed of new or revised policies and will be expected to read, understand and acknowledge the policies. Ask your supervisor for details of any specific policies or procedures that relate to your work.

Safeguards:

The law requires healthcare providers to implement and maintain appropriate safeguards to protect PHI from unauthorized access, use and disclosure. Some safeguards that are implemented through policy and are applicable to you include:

- Never look at or access a client's record if you do not have permission and a business need to do so. Access to electronic client records is logged by the system and monitored by the County Health and Human Services IT and Compliance programs. Unauthorized access is reported.
- Never discuss a client (even the existence of a client) with anyone outside of the authorized treatment or operations team. This unauthorized disclosure is one of the most common and often the most damaging forms of a breach.
- Always create strong passwords for system access and never share any of your passwords with anyone. Do not ask others to use their passwords. Follow the Security policy regarding this.
- Always lock your computer, using Ctrl + Alt + Delete or Windows key + L, when you leave it unattended. Ensure no one can watch you logon and that your screen is cannot be seen by unauthorized individuals when displaying confidential information.
- Ensure your computer automatically locks after a period of time that the commuter has not been in use. Follow the Security Policy regarding this.
- Safeguard the placement of laptops, computers and printers to limit potential access by unauthorized users. Retrieve documents from printers and faxes right away.
- Do not open suspicious attachments to e-mails, they may contain viruses or malware intended to steal confidential information or password credentials. Do not download or install software on county property without permission from the County Information Security Officer or HHS Technical Services. Call HHS Technical Services or e-mail the helpdesk for guidance or to report suspicious attachments or e-mails.
- Verify the identity of anyone requesting confidential information. If discussing PHI over the phone, ask identifying questions that the client would know (for example, last 4 of SSN, middle name, address etc..) to verify the identity of the caller.
- You must be completely familiar with all policies pertaining to storage of PHI or other confidential information prior to accessing that information. Do not store any confidential information on personal devices.
- Ensure all confidential information in paper form is in your control or is locked in a secure location where it can be accessed only by authorized users. Dispose of confidential paperwork by shredding or placing them in locked confidential recycle bins.
- All electronic communication should include a confidentiality statement.
- All PHI sent via e-mail to a non-county e-mail address (@marincounty.org) must be encrypted by typing the word "Encrypt" in the subject line. Never include confidential or individually identifiable information in the subject line of an e-mail. The subject line is not encrypted.
- You must ensure that any PHI or PII transmitted electronically (e-mail, Fax, voicemail) is appropriately protected, (only leave a call back message on voicemail), and you should double-check the addressee before sending a fax or e-mail. Failure to do so is one of the most common reasons for a breach. Call ahead to the recipient of the information to verify the fax number or e-mail address.
- Be aware of your surroundings when having conversations involving confidential information. Do not have confidential conversations in hallways or breakrooms. If possible, take your conversation to a confidential area/space. Remember an overheard conversation can still be a breach.
- Always report suspected or actual violations of policy or law that involve compliance, privacy or security. Reporting is not only required, if known, but is simply the right thing to do for all of us.

The Complaint Process

During the course of your work, you may be asked by a client how to submit a complaint about a perceived privacy violation or other matter concerning healthcare compliance. In addition, you may need to report an incident about a suspected breach that you think you may have committed or an incident involving others.

Client Complaints or Reports:

If a client has a concern or wants to make a complaint about an issue related to the County of Marin's actions relating to their health or confidential information, you should refer them to your supervisor. However, you may also refer them to the HHS Compliance and Privacy Program. If the client would like to remain anonymous, you should refer them to the **Confidential Compliance Line (415) 473-6948** or the client may e-mail HHSCompliance@marincounty.org. This information is also included in the Health & Human Services' Notice of Privacy Practices.

Employee or Contractor Complaints or Reports:

Workforce members, including contractors are required by law and by county policy to report any suspected or actual breach they may become aware of. This includes privacy and security incidents and breaches made by yourself or other employees, either accidentally or negligently.

To report a privacy or security incident or breach you should work with your supervisor or manager to complete HIPAA Form 1 - Privacy or Information Security Incident/Suspected Breach Report. If that is not reasonable or appropriate, you can contact the Compliance and Privacy Program Office directly. Reports may be made by phone, email or in-person.

Information You Should Know

If you need information about confidentiality and privacy practices, you can email the Compliance and Privacy Program Office at HHSCompliance@marincounty.org.

The HHS Compliance, Privacy and Security Officer is:
Rosanna Lallana – (415) 473-2531, rlallana@marincounty.org

The County Chief Information Security Officer is:
Jason Balderama (415) 473-7827, jbalderama@marincounty.org

The Confidential Compliance and Privacy Line is (415) 473-6948

CONFIDENTIALITY STATEMENT

General Use:

It is the legal and ethical responsibility of all County employees, contractors and volunteers to use personal and confidential client, employee and County business information (referred to collectively as "Confidential Information") in accordance with the law, County policy, and/or contract, and to preserve and protect the privacy rights of the subject of the information as they perform their County duties.

Confidential Information includes, but may not be limited to, any information that identifies an individual, written records or electronic records contained in systems to which employees, volunteers, interns and/or contractors, have been provided access.

Laws and regulations controlling the privacy of, access to and maintenance of confidential information include, but are not limited to, the following : Health Insurance Portability and Accountability Act (HIPAA), California Information Practices Act (IPA), California Confidentiality of Medical Information Act (CMIA), Lanterman-Petris-Short Act (LPS) and Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2). These and other laws apply whether the information is held in electronic or any other form or format, and whether the information is used or disclosed orally or in writing. County of Marin policies that control the way confidential information may be used include, but are not limited to, the following: County Personnel Management Regulations (PMRs), County of Marin Administrative Regulations, HHS Department policies and applicable Bargaining Unit agreement provisions.

Confidential information may be used and disclosed only in the performance of assigned duties for the purpose of providing services.

Unacceptable/Inappropriate Use:

Workforce members and contractors may not share or disclose confidential information with unauthorized individuals including, but not limited to, family, friends, acquaintances, or other County employees without the written authorization for disclosure from the client, unless the disclosure is specifically permitted under the regulations.

Enforcement Policies:

For employees, disciplinary action may be taken in accordance with PMRs, up to and including termination, if a client's confidentiality is violated in accordance with the laws, regulations, or County policies. For other workforce members and contractors, action will be taken, up to and including terminating the relationship and services, if a client's confidentiality is violated. In addition, individuals may subject themselves to individual civil or criminal prosecution for any such legal violations.

Privacy and Security Safeguards:

- To protect the privacy, confidentiality and security of all records retained by the County, including but not limited to, program records or data systems that employees have been provided access to in order to perform your assigned duties.
- To access, use, or disclose confidential information only in the performance of assigned duties, and when required or permitted by law. When disclosing confidential information, only the minimum information necessary, and only to persons who have the right to receive that information.
- To discard any confidential information by personally shredding or by discarding it in designated locked shredding containers.
- Login, User ID or password is not to be shared with anyone. Belief that someone else has used your Login, User ID or password, shall be immediately reported to your supervisor, and submit the Privacy/ Information Security Incident/Breach Report to the Compliance and Privacy Program Office.
- Computers are to be locked when leaving the workstation to prevent unauthorized access to confidential information.
- Access to all electronic information systems is subject to audit in accordance with Federal and State mandates and County policy.
- Safeguarding confidential information acquired in the course of employment continues after termination of employment or service.

Questions regarding Confidentiality policies applicable to your job, including policies for use and disclosure, and for safeguarding the security and privacy of confidential information should be directed to your supervisor and/or the Compliance and Privacy Program Office.

Check all that apply:
[ ] I acknowledge receipt of the "Confidentiality and Privacy in Health and Human Services" which provides information and guidance on PHI/PII use and disclosures.
[ ] I have read the provisions of the Confidentiality Statement pertaining to General Use, Unacceptable Use, and Enforcement Policies.

I understand and agree to comply with the obligations relating to the privacy and security of confidential information.

_____
Print Name

_____ _____
Signature Date

_____ _____
County Department Division

Check One: [ ] Employee [ ] Temporary Employee
[ ] Volunteer [ ] Consultant/Contractor
[ ] Intern [ ] Other _____