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

Grant Nash Colfax, MD, Director
Department of Health and Human Services

Confidentiality and Privacy in Healthcare

As employees of a healthcare system, 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, other personal information about clients or consumers, 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 enter, access or use information that is considered to be California State "Department PII". It is critically important that you protect any confidential information that should not be disclosed 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 detailed in the County Personnel Management Regulations (PMRs). Our collective effort to ensure the privacy and security of confidential information upholds our 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 created 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 regulations govern who has access to Protected Health Information (PHI). They ensure that PHI is used appropriately by creating a national minimum standard of privacy (State laws can be more stringent). The privacy regulations also give clients specific rights regarding their own health information.
- **Security:** The security regulations govern how health information, in electronic format, is protected. They establish safeguards for Protected Health Information.

While we regularly refer to HIPAA regulations, other state and federal regulations govern the privacy and security of health information and other personal information. These regulations are the ones that most often regulate our County work: 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) – Personally Identifiable Information (PII)

PHI is information related to an individual's health care treatment and/or to 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, 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. PII is similar to PHI and must also be protected. PII differs from PHI in that it does not combine personal information with health information.

- **Client identifiers:** Names, Street address, city, county, full zip code (with some qualifications), dates directly related to an individual (e.g. birth date, dates of service), telephone and fax numbers, email addresses, social security numbers, credit card numbers, medical record or enrollment numbers, account numbers, certificate/license numbers, vehicle identifiers, Internet Protocol (IP) addresses, biometric identifiers (e.g. finger prints), full-face images, 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.

Use of PHI/PII:

Employees 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. When used properly, PHI supports positive outcomes in the healthcare services we provide. 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.

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 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 professional 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. Permitted disclosures without authorization may include: discussing a client's own information with, or providing a copy of the information t, the client. Healthcare providers may also 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 policies regulations that apply to your area of work, prior to disclosing any confidential information. In addition, always ask your supervisor or the Privacy Officer for guidance if you are unsure about the permitted reasons for disclosures.

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 authentic 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 Intranet. 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 available 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 Security Officer or HHS IT. Call HHS IT 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 ensure you recognize the client's voice or you ask identifying questions that the client would know (for example, last 4 of SSN, middle name, address etc..).
- 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. This 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 break-rooms. 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 health services, you should refer them to your supervisor. However, you may also refer them to the HHS Compliance and Privacy Program staff listed below. If the client would like to remain anonymous, you should refer them to our 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 Complaints or Reports:

If you need to report a suspected breach or if you want information about confidentiality and privacy practices, you should work with your supervisor or manager. If that is not reasonable or appropriate, you can call the Compliance and Privacy Program staff at any of the numbers below. Reports may be made by phone, email or in-person.

Please remember, employees are required by law and by county policy to report any breach or suspected breach they may become aware of. This includes breaches made by yourself or other employees, either accidentally or negligently.

Information You Should Know

You should know who is, and how to contact, the Compliance, Privacy and the Security Officer for your area of work.

The Compliance, Privacy and Security Officer for HSS is:
David Rothery – (415) 473-2087, drothery@marincounty.org – 20 N. San Pedro Rd.

The Deputy Compliance, Privacy and Security Officer for HHS is:
John Bhambra – (415) 473-2531, jbhambra@marincounty.org – 20 N. San Pedro Rd.

The County Security Officer is:
Jason Balderama (415) 473-7827, jbalderama@marincounty.org – located at 1600 Los Gamos.

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