SFDPH
Annual Privacy and Data Security Training Module

FY2017 - 2018
Objectives

By the end of this course you will demonstrate:

1. How HIPAA privacy rules protect the privacy and security of our patient/client/resident’s confidential information

2. What your responsibilities are for using and protecting health information (PHI), including using electronic devices

3. How to report an actual or suspected Privacy Breach
Why We Care about Privacy

How would you feel if:

• Staff at your physician’s office gossiped about your medical condition?

• Someone checking you in at your clinic asked why you were there?

• Your local hospital lost a laptop containing unencrypted information including:
  • Your social security number?
  • Your address?
  • Your phone number?
  • Your medical information?
What is HIPAA and TPO?

HIPAA is the Health Insurance Portability and Accountability Act and is a federal privacy law that:

Protects patient privacy and allows sharing of health information for the purposes of **TPO**:

- **Treatment**
- **Payment** (billing and insurance processing)
- **Operations** (care coordination, analyses, audits and quality management)
Minimum Necessary

• HIPAA requires that information sharing be kept to the minimum amount of information necessary to do our jobs – this is known as the “minimum necessary” rule

• Sharing of PHI should be limited to those who “need to know”
As a DPH workforce member, you are responsible for following policies and procedures to protect patient privacy and maintain the security of information.

Ask your supervisor or manager for guidance.

Remember that privacy applies to ALL verbal, written, and electronic information.
What Patient Information Must We Protect?

SFDPH must protect every individual’s information that includes at least one of the 18 personal identifiers in association with health information

Health Information + Identifiers =

*Protected Health Information (PHI)

*PHI Examples: Names of attendees at a therapy group, a patient’s registration form

BREACH DEFINITION: An unauthorized acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by HIPAA, which compromises the security or privacy of such information, and poses a significant risk of financial, reputational, or other harm to the affected individual
**Protected Health Information (PHI)**

PHI is information that can be individually identified as belonging to a particular person either living or dead including:

<table>
<thead>
<tr>
<th>✓ 18 Identifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Name</td>
</tr>
<tr>
<td>✓ Postal Address</td>
</tr>
<tr>
<td>✓ License numbers</td>
</tr>
<tr>
<td>✓ Telephone numbers</td>
</tr>
<tr>
<td>✓ Fax numbers</td>
</tr>
<tr>
<td>✓ Email address</td>
</tr>
<tr>
<td>✓ URL address</td>
</tr>
<tr>
<td>✓ IP Address</td>
</tr>
<tr>
<td>✓ Medical record number</td>
</tr>
</tbody>
</table>
Medical Privacy Laws

SFDPH and its contractors must also follow California medical privacy laws. **Snooping is not allowed!**

**WE AUDIT!**

To avoid snooping, note the following:

- Do NOT look in the health record of someone who is not under your care or you do not have a business need
- Do NOT look at a family member’s or a friend’s health record
- Do NOT look at your own medical record (per DPH Policy)

Unauthorized access is a serious offense and can lead to **loss of employment, fines and licensure sanctions**

Office of Compliance and Privacy Affairs (OCPA)
California Medical Privacy Laws

PLEASE NOTIFY YOUR SUPERVISOR & PRIVACY OFFICER IMMEDIATELY IF YOU SUSPECT A BREACH OF PRIVACY

HOTLINE (855) 729-6040

- In certain situations, we must report a breach to the State within 24 hours
- Hospitals must report any suspected breach to the California Department of Public Health within 15 business days
- DPH Contractors and CBOs must notify DPH immediately of a suspected breach
Examples of Privacy Breaches

• Unencrypted electronic devices (laptops, smart phones, flash drives) containing PHI stolen from vehicles, homes, businesses or public transit

• Unauthorized patient information posted on social media

• Disclosing PHI (such as a diagnoses) when family members, friends, media or other unauthorized people are present
Fines and Penalties

• **HIPAA Criminal Penalties:** $50,000 to $1,500,000 fines and imprisonment up to 10 years

• **HIPAA Civil Penalties:** $100 - $25,000 per year fines and more fines if multiple year violations

• **State Laws & Penalties apply to institutions and individuals:**
  • Fines up to $250,000
  • May impact professional licensure
  • Potential imprisonment up to 10 years

• **Employees:** Disciplinary actions up to termination
Notice of Privacy Practices

- Every patient must be provided with the SFDPH “Notice Of HIPAA Privacy Rights” upon first visit.
- Acknowledgment of receipt is filed in the medical record.
- Clients of Behavioral Health must also be offered the notice annually thereafter.
- Posters are to be displayed in common areas, [Link] for ordering posters & notices.

SDPH Summary Notice of HIPAA Privacy Rights and Acknowledgement of Receipt

Full Notice: You have been provided the full notice of HIPAA Privacy Rights. Please read it carefully. You can also find it at https://www.sdpdh.org/about/sdphpg/essentials/mediacy/hipaa-hipaanotices.asp.

Who will follow the rules in this notice: All SDPH and contract provider employees, SDPH affiliates, as well as staff assigned to SDPH by the University of California at San Francisco, must follow these rules.

You have the right to:
- Access or obtain a copy of your health record (charges may be necessary).
- Consent to use or disclose your health record for treatment, payment, and operations purposes.
- Be informed about the purposes for which your records will be used.
- Be informed that your health record will not be used for research purposes.
- Be informed about the procedures for donating or rejecting your health record.
- Be informed about the methods used to protect your health record.
- Be informed about the procedures for filing a complaint.

Office of Compliance and Privacy Affairs (OCPA)
• The Designated Record Set includes a patient’s medical record, radiology images, copied documents from other health institutions, etc. It can be paper, electronic or both

• The Designated Record Set is the property of the SFDPH; BUT patients can request a copy of any part or all of their health record

• **DO NOT** give out any part of the Designated Record Set on your own. Refer the patient/client to the Medical Records Department at your location
## DPH Privacy Policy Matrix – Sharing PHI for Treatment Reasons

<table>
<thead>
<tr>
<th>Description of PHI</th>
<th>Who may disclose it?</th>
<th>Who may receive it?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Health</strong>*</td>
<td>General Health Provider</td>
<td>Patient’s providers and providers’ staff for the purpose of treatment, diagnosis, or referral</td>
</tr>
<tr>
<td><strong>Mental Health</strong>*</td>
<td>Mental Health Provider</td>
<td>Any healthcare provider (any discipline) &quot;who has medical or psychological responsibility for the patient&quot;</td>
</tr>
<tr>
<td><strong>Drug/Alcohol Treatment Program</strong>*</td>
<td>Drug/Alcohol Treatment Program Provider</td>
<td>Only another member of the client's treatment team WITHIN the specific drug/alcohol treatment program</td>
</tr>
<tr>
<td><strong>HIV/AIDS CCSF Health Service Provider Network</strong>*</td>
<td>HIV/AIDS CCSF Health Service Provider</td>
<td>Only another HIV Health Service provider who registers client in ARIES database</td>
</tr>
</tbody>
</table>

*including knowledge of mental health, substance use, HIV/AIDS, STDs
When discussing patient’s/client’s Personal Health Information when family and friends are present, providers should:

- Ask for the patient’s permission to discuss his or her health information in front of others
- Offer the patient an opportunity to object before sharing
- Document verbal permission in the medical record
Note: For certain situations involving mental health, substance use disorder, sexually transmitted disease, HIV/AIDS, or developmental disabilities, providers should:

• Seek patient/client specific prior written authorization to disclose PHI in front of a family member, friend or caregiver
Best Practices to Maintain Privacy

Handling paperwork and voicemail:

• Double check any paperwork to make sure that you are giving information to the correct patient

• Be aware of handling patient information and avoid accidentally leaving paperwork where it shouldn’t be

• When leaving a voicemail for a patient, just provide the minimum info – your name, clinic and phone number
Data Security: Good Computer Practices

• Ensure your computer and data are physically secured by using locked drawers and placement in a secured area

• Log off your computer terminal when you are done or even if you walk away for a few moments

• Ensure information on computer screens are not visible to someone passing by
Data Security: Passwords

• Create a strong password – use capitals, symbols and numbers

• Password data should not be stored where unauthorized people may discover it (e.g. Post-it, calendars, near computer or devices)

• One Account/One User- do not share your username or password with anyone

You are responsible for protecting DPH data, information, workstations, and portable electronic devices used in your job from loss, damage or misuse. Before you transport PHI offsite, you must:

• Obtain prior authorization from your manager

• Your portable device (e.g., smartphone, laptop, tablet, etc.) must be encrypted

• Keep all PHI on your person and in your possession at all times
Data Security: PHI Access and Disclosure

- All access attempts to SFDPH systems are subject to monitoring, auditing and penalties if unauthorized.

- Always use the SFDPH cover sheet when faxing or mailing PHI (see right).

- Discard documents with PHI only in the confidential bin/shredder (never discard in the trash or recycle bin).
Data Security: Email Communication

• **Always** type the word **Secure** in the subject line for any email containing PHI  *(RAMS Note: This only applies for those with sfdph.org or sfgov.org email addresses)*

• **Always** confirm email addresses *before* sending PHI

• **Always** use the official confidentiality statement as a permanent signature statement for all of your emails

• **Never** put personal identifiers of a living or deceased client in the subject line of an email

• **Never** email PHI to distribution lists
If you participate in **social media**, remember:

- PHI postings or hyper-linking to photos, images, videos, recordings, texts, etc., of unauthorized information that could reasonably lead to the identification of a client/patient is **prohibited**

- The above actions may subject you to disciplinary action (up to and including termination) and individual fines/sanctions which could impact your professional license

- **Text messages** cannot be encrypted; do not text PHI unless authorized by a Supervisor/Privacy Officer
Electronic Recording is Prohibited

We are committed to protecting the privacy of our patients and clients.

Please do not photograph, video tape, or audio record in this Department of Public Health facility without prior authorization.


Approved 8/24/15 – SF Department of Public Health – Office of Compliance and Privacy Affairs, compliance.privacy@sfdph.org, Toll-free Hotline: 1-855-729-6040
Cybersecurity – Phishing

- **Phishing** is an attempt to obtain sensitive information such as usernames or passwords by masquerading as a trustworthy entity in an electronic communication.

- Phishing attempts can also include delivering an attachment with malware or direct the user to a fraudulent website containing malicious code.

- **Malicious links** can infect your computer and the network or take you to web pages designed to steal your data and DPH data.
Cybersecurity – Phishing Awareness

- **STOP:** Do you really need to view/open a suspicious email?

- **THINK:** Never provide your login information or password to an email request. DPH will never ask for this information.

- **When in doubt, “throw it out”** - delete emails and avoid web page links that look suspicious.
Complaints and Breaches

PLEASE NOTIFY YOUR SUPERVISOR & PRIVACY OFFICER IMMEDIATELY IF YOU SUSPECT A BREACH OF PRIVACY

• You may also report anonymously (SFDPH has a non-retaliation policy for employees who register complaints)

SFDPH Privacy Toll-Free Hotline: 1-855-729-6040

Email: compliance.privacy@sfdph.org

Hotline poster is available here

• Report lost or stolen electronic devices to your immediate supervisor and call the SFDPH Helpdesk: 415-759-3577
<table>
<thead>
<tr>
<th>NAME</th>
<th>REPRESENTING</th>
<th>PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maggie Rykowski</td>
<td>Director, Office of Compliance &amp; Privacy Affairs</td>
<td>(855) 729-6040</td>
</tr>
<tr>
<td>Heather Zalatimo</td>
<td>Data Security</td>
<td>(415) 759-3577</td>
</tr>
<tr>
<td>Deborah Sherwood</td>
<td>Approvals for non-hospital-based research</td>
<td>(415) 255-3435</td>
</tr>
<tr>
<td>Garrett Chatfield</td>
<td>Laguna Honda Hospital and Rehabilitation Center</td>
<td>(415) 759-4072</td>
</tr>
<tr>
<td>Maggie Rykowski</td>
<td>Zuckerberg San Francisco General Hospital Campus</td>
<td>(415) 206-4294</td>
</tr>
<tr>
<td>Josh Jacobs</td>
<td>Department of Homelessness &amp; Supportive Housing</td>
<td>(415) 557-6035</td>
</tr>
</tbody>
</table>

• Link to official SFDPH cover sheet for ALL faxes and mail: https://www.sfdph.org/dph/files/HIPAAdocs/PrivacyPolicies/FormPHICvrSht4FaxInterofficeyMailAdopted05132010.pdf

• SFDPH Email confidentiality statement to copy and paste to permanent signature line: “This e-mail is intended for the recipient only. If you receive this e-mail in error, notify the sender and destroy the e-mail immediately. Disclosure of the PHI contained herein may subject the discloser to civil or criminal penalties under state and federal privacy laws.”
RAMS Privacy Officer

- Angela Tang, RAMS Director of Operations
- Contact Info: (415) 800-0699 ext. 200 / angelatang@ramsinc.org

Media Contact:

- You must consult with RAMS Privacy Officer before speaking to the press

Research Involvement:

- All research activity requests are to be directed to RAMS Privacy Officer
- Research activities include, but are not limited to, posting of research study flyer, outreach & promotion of study at programs, targeted client recruitment, etc.
Additional Related RAMS Policies and Protocols:

Please refer to full policy/protocol description

* **HIPAA Record Request Log:** Each program maintains a log which tracks any and all medical record requests (refer to program-specific procedure)

* **Contact with Legal Entities:** Any and all contact with legal entities must first be discussed with supervisor and program/clinic director (may be in consultation with RAMS Privacy Officer) before responding to any requests. This includes record requests that may include an Authorization to Release Information.

* **RAMS Policy & Procedure on Maintenance and Use of Psychotherapy Notes and Informal Memory Prompts:** Provides guidance regarding creation, use, and the subsequent maintenance of psychotherapy notes/informal memory prompts separate and apart from the medical record, and the proper means to destroy any notes that include Protected Health Information.
Additional Related RAMS Policies and Protocols (cont...)

- **RAMS Policy & Procedure on HIPAA Compliance: Reporting of Unlawful or Unauthorized Access of Protected Health Information:** All staff must report unlawful or unauthorized access of Protected Health Information. Pursuant to state laws, RAMS strictly prohibits inappropriate viewing of protected patient health information.

- **RAMS Policy & Procedure on Whistleblower:** If any employee reasonably believes that some policy, practice, or activity of RAMS is in violation of law, a written complaint may be filed by that employee with the Director of Human Resources. Complaints can also be directly reported to the California State Attorney General’s Whistleblower Hotline.
When in doubt, seek consultation!
Next Steps

In order to complete and receive credit for the Annual Privacy and Security training, you MUST:

1. Take and pass the Annual Privacy Quiz (return to the “Online Event Registration” page). 100% accuracy required. Certificate will be printable after passing the quiz.

2. Read and electronically sign the “User Confidentiality, Security, and Electronic Signature Agreement”

2. Email Certificate and electronically signed User Agreement to compliance@ramsinc.org
RAMS values client privacy as an important part of our mission to provide community based, culturally-competent, and consumer-guided comprehensive services.

Thank you for helping us protect the privacy and security of our clients and staff.