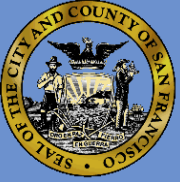


SFDPH

Annual Compliance and Privacy

Training Part 2

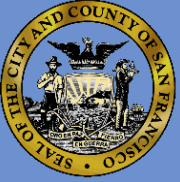
FY 24-25



Privacy Objectives

By the end of the privacy component you will demonstrate:

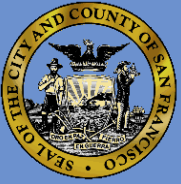
1. How privacy rules protect the privacy and security of our patient/client/resident's confidential information
2. What your responsibilities are for using and protecting health information (PHI), including using electronic devices
3. How to report an actual or suspected Privacy Breach



Why We Care About Privacy

How would you feel if:

- Staff at your physician's office gossiped about your medical condition?
- Your personal information including social security number was stolen from a backpack in your provider's car?
- A non-profit you donated to lost a laptop containing unencrypted information including:
 - Your social security number?
 - Your date of birth?
 - Your phone number?



Laws Governing Privacy and Security

HIPAA is the most well-known law governing health care privacy. There are many other Federal and State Laws that also protect govern our health care privacy practices.

Other Laws, like the **HITECH Act** which set privacy and data security requirements for electronic health records, and the **California Medical Information Act**, which protects patient privacy, are also important to know.

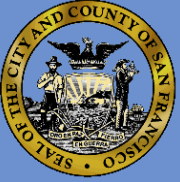
Federal Laws

- Health Insurance Portability and Accountability Act – HIPAA
- HITECH Act
- 42 CFR Part 2

State Laws

- California Medical Information Act
- Health Care Facilities Data Breach law
- Patient Access to Health Records Act – PAHRA

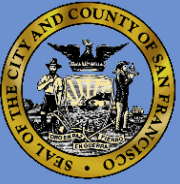




DPH Policies and Procedures

- As a DPH contractor, **you are responsible** for following policies and procedures to protect client/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**

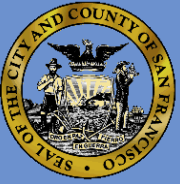




What Patient Information Must We Protect?

SFDPH must protect every individual's information that includes at least one of 18 personal identifiers in association with healthcare information

**Health Information + Identifiers =
*Protected Health Information (PHI)**

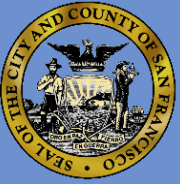


Protected Health Information

PHI also include at least one of the personal **identifiers** listed below.

✓ 18 Identifiers

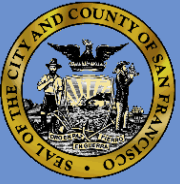
✓ Name	✓ Social Security Number (SSN)
✓ Postal Address	✓ Account numbers
✓ License numbers	✓ All elements of dates, except year
✓ Telephone numbers	✓ Health plan beneficiary numbers
✓ Fax numbers	✓ Device identifier and their serial numbers
✓ Email address	✓ Vehicle identifiers and serial numbers
✓ URL address	✓ Biometric identifier (finger and voice prints)
✓ IP Address	✓ Full face photo and other comparable images
✓ Medical record number	✓ Any other unique identifying number, code, or characteristic



Protected Health Information

Protected Health Information is

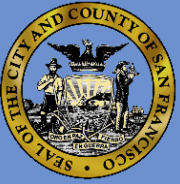
- Information used to identify a patient
 - LIVING OR DECEASED
- Related to past present or future condition
 - Biological
 - Psychological
 - Social
- Related to healthcare services including:
 - Services Provided
 - Payment for Services



Protected Health Information

Examples of Protected Health Information (PHI)

- Sign-in sheet for a group therapy session
- Patient names and immunization status from a research study
- Patient bill
- Authorization for services form

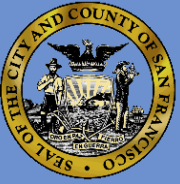


What is HIPAA and TPO?

HIPAA

Protects patient privacy **and** allows sharing of health information **without authorization** for the purposes of **TPO**:

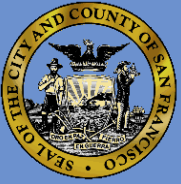
- **Treatment**
 - Exchanging information with other providers to provide care to patients
- **Payment**
 - Billing and insurance processing
- **Operations**
 - Refers to financial, legal, and administrative activities that are necessary to run SFDPH or a healthcare organization
 - Teaching students, interns, and residents
 - Performing audits



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”**
- Example: A clinic employee who works in registration, only needs to access patient insurance and demographic information, **and not** the patient’s behavioral health history

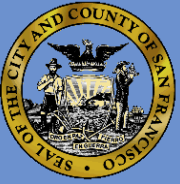




Privacy Breach



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**

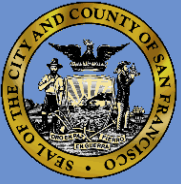


Privacy Breach: Reporting

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

HOTLINE (855) 729-6040

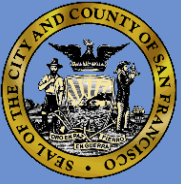
- If privacy incident is related to SUD and behavioral services, we must report a breach to the State as soon as possible
- DPH Contractors and Community Based Organizations (CBO) must notify DPH immediately of a suspected breach



Privacy Breach: Examples

- Unencrypted electronic devices (laptops, smart phones, flash drives) containing PHI stolen from vehicles, homes or public transit
- Staff not involved in client's case discussing situation with co-workers or friends
- Case file left on public transit





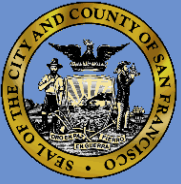
Privacy Breach: Unauthorized Access

DPH employees, and contractors must follow DPH policy and medical privacy laws.

Unauthorized access is not allowed!



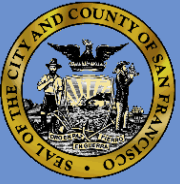
- Deliberately looking at anyone's medical records, including your own, if it is not part of your assigned job duties is called an unauthorized access.
- Just because an EHR allows you to access a record, doesn't mean the access is authorized.
- Unauthorized access is a serious violation of a person's privacy and can lead to discipline including separation



Privacy Breach: Unauthorized Access

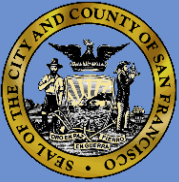
To avoid unauthorized access, note the following:

- 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)



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

Describes patient privacy rights and how SFDPH can use, and share, PHI.

- 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



NAME
DOB
MRU

SFDPH Summary Notice of HIPAA Privacy Practices and Acknowledgement of Receipt

Full Notice: You have been provided the Full Notice of HIPAA Privacy Practices. Please read it carefully. You can also find it at: <https://www.sfdph.org/dph/comupg/oseservices/medsvs/HIPAA/HIPAAsummaries.asp>.

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

You have the right to: (Please see possible restrictions in the “Full Notice of Privacy Practices”.)

- Ask to see, read and/or obtain a copy of your health record (charges may be necessary).
- Ask to correct information that you believe is wrong in your health record.
- Ask that your health information not be shared with certain individuals.
- Ask that your health information not be used for certain purposes; for example, research.
- Ask that copies of your health record be sent to someone (charges may be necessary).
- Be informed about who has read your record (for reasons other than treatment, payment and program improvement purposes).
- Specify where and how DPH employees may contact you.

DPH may use and disclose your health information to improve your treatment.

- To improve the quality of care you receive, health information may be shared between treatment providers, including your health information regarding mental health, substance abuse, HIV/AIDS, sexually transmitted diseases (STD), and developmental disabilities.
- There are circumstances when health information about you will not be shared unless you first give your permission for it to be shared; such as services received in substance abuse treatment agencies.

If you believe your privacy rights have NOT been maintained while receiving DPH services, you may file a complaint. If you have concerns about how your health information might be (or has been) shared, please speak with your provider or contact either of the following: (1) Secretary of U.S. Dept. of Health and Human Services, Office of Civil Rights, Attn: Regional Manager, 50 United Nations Plaza, Rm. 322, San Francisco, CA 94103. (2) DPH Office of Compliance and Privacy Affairs, 101 Grove St., Room 330, San Francisco, CA 94102, or call toll-free 1-855-729-6040. You will not be penalized in any way for filing a complaint.

I acknowledge receipt of the SF Department of Public Health “Full Notice of HIPAA Privacy Practices.”

SIGNATURE OF PATIENT/RESIDENT/CLIENT OR THEIR REPRESENTATIVE		DATE
PRINT NAME	IS REPRESENTATIVE, SPECIFY RELATIONSHIP	IS REPRESENTATIVE APPLICABLE

STAFF/WITNESS: If written acknowledgement is NOT obtained, please complete the following:


<input type="checkbox"/> Unable to sign <input type="checkbox"/> Declined to sign <input type="checkbox"/> Other, Describe:		DATE
PRINT NAME	DEPARTMENT/ORG	

(Rev. 5/22/12) SFDPH Office of Compliance and Privacy Affairs



Notice of Privacy Practices

- Authorizes sharing of health information
- The right to restrict who receives health information
- The right to request confidential communication
 - Only receive confidential communication at his/her work phone number



NAME
DOB
MRU

San Francisco Department of Public Health

SFDPH Summary Notice of HIPAA Privacy Practices and Acknowledgement of Receipt

Full Notice: You have been provided the Full Notice of HIPAA Privacy Practices. Please read it carefully. You can also find it at: <https://www.sfdph.org/dph/comupg/oservices/medsvs/HIPAA/HIPAAsummaries.asp>.

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

You have the right to: (Please see possible restrictions in the "Full Notice of Privacy Practices".)

- Ask to see, read and/or obtain a copy of your health record (charges may be necessary).
- Ask to correct information that you believe is wrong in your health record.
- Ask that your health information not be shared with certain individuals.
- Ask that your health information not be used for certain purposes; for example, research.
- Ask that copies of your health record be sent to someone (charges may be necessary).
- Be informed about who has read your record (for reasons other than treatment, payment and program improvement purposes).
- Specify where and how DPH employees may contact you.

DPH may use and disclose your health information to improve your treatment.

- To improve the quality of care you receive, health information may be shared between treatment providers, including your health information regarding mental health, substance abuse, HIV/AIDS, sexually transmitted diseases (STD), and developmental disabilities.
- There are circumstances when health information about you will not be shared unless you first give your permission for it to be shared; such as services received in substance abuse treatment agencies.

If you believe your privacy rights have NOT been maintained while receiving DPH services, you may file a complaint. If you have concerns about how your health information might be (or has been) shared, please speak with your provider or contact either of the following: (1) Secretary of U.S. Dept. of Health and Human Services, Office of Civil Rights, Attn: Regional Manager, 50 United Nations Plaza, Rm. 322, San Francisco, CA 94103. (2) DPH Office of Compliance and Privacy Affairs, 101 Grove St., Room 330, San Francisco, CA 94102, or call toll-free 1-855-729-6040. You will not be penalized in any way for filing a complaint.

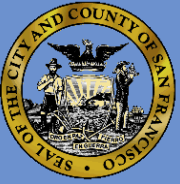
I acknowledge receipt of the SF Department of Public Health "Full Notice of HIPAA Privacy Practices."

SIGNATURE OF PATIENT/RESIDENT/CLIENT OR THEIR REPRESENTATIVE		DATE
PRINT NAME	IS REPRESENTATIVE, SPECIFY RELATIONSHIP	INITIALS IF APPLICABLE

STAFF/WITNESS: If written acknowledgement is NOT obtained, please complete the following:

<input type="checkbox"/> Unable to sign <input type="checkbox"/> Declined to sign <input type="checkbox"/> Other, Describe:		DATE
PRINT NAME	DEPARTMENT/ORG	

(Rev. 5/22/12) SFDPH Office of Compliance and Privacy Affairs

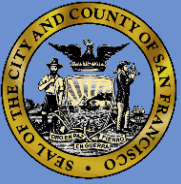


Designated Record Set



- The Designated Record Set (DRS) can be paper, electronic, or both, and includes a patient's
 - medical record
 - billing records
 - wellness and disease management notes
- The Designated Record Set is the property of DPH and/or CBO
- BUT patients have the right to access the PHI in their DRS
- Patients can request a copy of any part or all of their health records

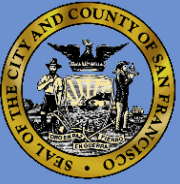
DO NOT give out any part of the Designated Record Set on your own. Refer the patient/client to the Medical Records Department at your location



Special Circumstances for Disclosures

When discussing client's Personal Health Information when family and friends are present, **providers should**:

- Ask for the client's permission to discuss his or her health information in front of others
- Offer the client an opportunity to object before sharing
- Document verbal permission in the medical record

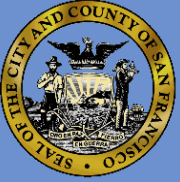


Permissible Disclosures

Permissible Disclosures: information that can be disclosed to others WITHOUT permission. Examples of permissible disclosures are:



- Public Health activities
 - Birth/death records
- Reporting/investigating *certain* diseases
- Reporting abuse and neglect
- *Certain* law enforcement activities
 - Court subpoena

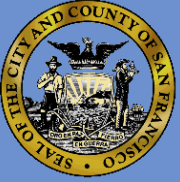


Special Circumstances for Disclosures

Client must give **specific prior written authorization** to disclose

- **Substance use disorder**
 - From a substance use disorder program
- **Uses other than treatment, payment or operations**
- **Reasons not prescribed by law**

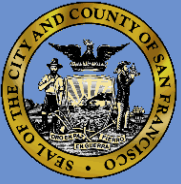




Best Practices to Protect Patient Privacy: Objectives

By the end of the best practices for privacy component you will demonstrate:

1. Understand the importance of protecting patient privacy in different job roles
2. Understand privacy principles as they relate to your daily work
3. Know practical tips for minimizing the risks of privacy breaches
4. Know how to get help with your privacy concerns

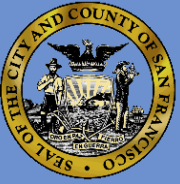


Best Practices to Protect Patient Privacy

Handling paperwork and voicemail

- Be aware of handling client information and avoid accidentally leaving paperwork where it shouldn't be
- When leaving a voicemail for a client just provide the minimum info – your name, organization name and phone number



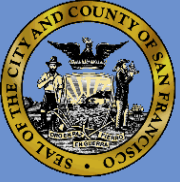


Best Practices to Protect Patient Privacy

Talking in Public Areas

- Remember where you are and who can overhear you
- Refrain from discussing client information in public areas such as a:
 - Hallway
 - Elevator
 - Reception Area
 - Public Space
- Whenever possible discuss PHI in a private area



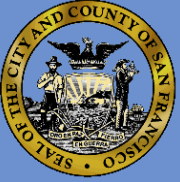


Best Practices to Protect Patient Privacy



Social Media

- 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 is **prohibited**
- The above actions may subject you to disciplinary action and individual fines/sanctions which could impact your professional license



Best Practices to Protect Patient Privacy

Text Messaging

- Sending PHI by text message is never allowed. You cannot use text messages to communicate about patients if the message contains PHI.
- You cannot send PHI to patients by text message. The most secure way to message patients is through their patient portal.
- For further guidelines on using electronic communications see the Sending Electronic Messages to Adult Patients.



Electronic Recording is Prohibited

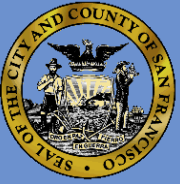


We are committed to protecting the privacy of our patients and clients.



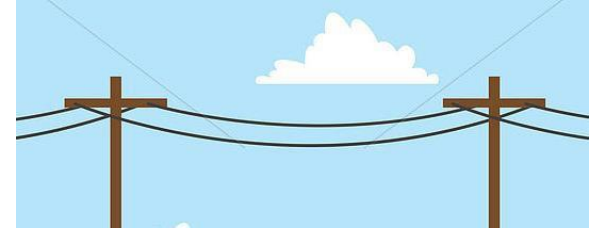
Please do not photograph, video tape, or audio record in this Department of Public Health facility without prior authorization.

Reference Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), 45C.F.R. Parts 160 & 164, Subparts A & E and California Penal Code Section 632
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

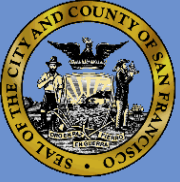


Best Practices to Protect Patient Privacy

Faxing/Mailing/E-mailing



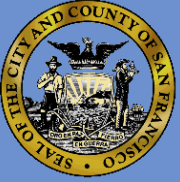
- **Always** Include the confidentiality cover sheet as the first page
- **Always** confirm fax number/address/e-mail addresses before sending PHI. Take a second before hitting “send.”
- **Always** use the official confidentiality statement as a permanent signature statement for all of your emails



Best Practices – Email



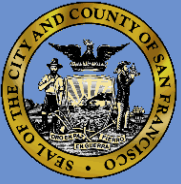
- If you accidentally send an email to someone, notify the sender to delete the message from their inbox and trash folder.
- Verify with the sender that it was deleted.
- Notify your supervisor, privacy officer or the SFDPH Office of Compliance & Privacy Affairs



Best Practices to Protect Patient Privacy

Faxing/Mailing/E-mailing/Printing

- **Never** email PHI to distribution lists
- **Immediately** pick up documents as soon as you print them
- **Immediately** delete documents with PHI from common scan folders or from your work computer's desktop



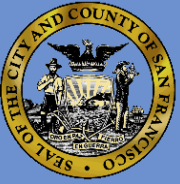
Best Practices to Protect Patient Privacy



Transporting PHI

Before you transport PHI:

- 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**
- **NEVER** leave devices or paperwork in your car or unattended

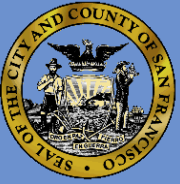


Best Practices to Protect Patient Privacy



Securing PHI

- Paper files should be store in a locked file cabinet in a locked room
 - 2 layers of security
 - Always lock up papers with PHI in files at the end of the day
- Ensure information on computer screens are not visible to someone passing by
 - Turning your monitor away from view or
 - Using a privacy screen
 - “Lock” your computer when you are away from your computer



Question and Breaches

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

- You may also report anonymously
- Report lost or stolen electronic devices to your immediately supervisor and Service Desk

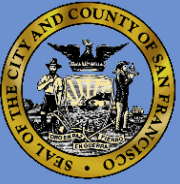
SFDPH Privacy Toll-Free Hotline: 1-855-729-6040

Email : compliance.privacy@sfdph.org

*****Please contact us with any questions.*****

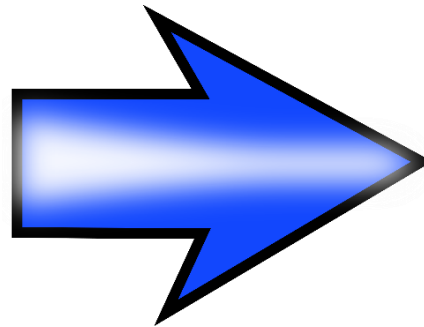
SFDPH Service Desk: 628-206-7378

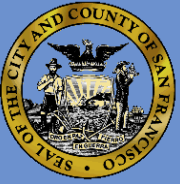




Data Security: Key Points

- If you are authorized to take PHI offsite, always keep PHI on you in a backpack or bag
- Ensure laptops, and other devices, are encrypted





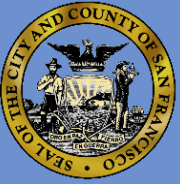
Data Security: Key Points

When sending email containing PHI:

- Encrypt **INTERNAL AND EXTERNAL** E-mails
 - Use your organization's e-mail encryption

***IF YOU CANNOT ENCRYPT E-MAIL DO NOT SEND PHI ELECTRONICALLY**

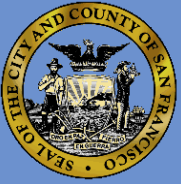
***Exception** – If the client insists on receiving unencrypted email, see the DPH Sending Electronic Messages to Adult Patients policy



Data Security: Key Points


- Never put PHI in the subject line
- Always confirm the e-mail address prior to sending
- Never use personal e-mail for work
- When working remotely, you need to protect PHI just as you were on-site. Saving files locally on your personal computer hard drive or cloud storage, or personal phone is not permitted. You are also prohibited from allowing family members to access computers with work files on them, or view any work related files or PHI.
- All work related files must be saved within DPH's remote desktop environment.





Data Security: PHI Access and Disclosure

- All access attempts to SFDPH systems are subject to monitoring, auditing and penalties if unauthorized
- Always use the DPH 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)



San Francisco Department of Public Health
City and County of San Francisco

Protected Health Information Cover Sheet
Required for
Fax Transmissions ~ Interoffice Mail ~ US Mail & Other Mail

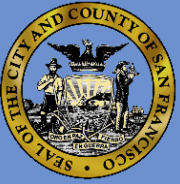
CAUTION

THE ATTACHED IS SOLELY FOR THE INTENDED RECIPIENT/PROGRAM. IT CONTAINS PROTECTED PRIVATE, PRIVILEGED OR PROTECTED HEALTH INFORMATION (PHI). IF YOU ARE NOT THE INTENDED RECIPIENT, ANY DISCLOSURE, COPYING, USE, OR DISTRIBUTION OF THE INFORMATION ATTACHED IS STRICTLY PROHIBITED AND MAY SUBJECT DISCLOSURE TO CIVIL OR CRIMINAL PENALTIES UNDER STATE AND FEDERAL PRIVACY LAWS. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, PLEASE NOTIFY THE SENDER IMMEDIATELY. THANK YOU.

RECIPIENT, PLEASE NOTE: PER FEDERAL SUBSTANCE ABUSE REGULATIONS [42 C.F.R. PART 2], DOCUMENTS CONTAINING PHI SENT TO YOU FROM A SUBSTANCE ABUSE TREATMENT PROGRAM MAY NOT BE RE-DISCLOSED WITHOUT SIGNED AUTHORIZATION FROM THE CLIENT.

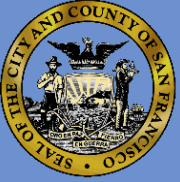
DATE SENT:	If Fax, Total # of Faxed Pages (including this cover page):
<u>FROM SENDER</u>	<u>TO RECIPIENT</u>
Name:	Name:
Program:	Program:
Dept/Agency:	Dept/Agency:
Street Address:	Street Address:
City/State/Zip:	City/State/Zip:
Phone:	Phone:
Fax:	Fax:

051410 DPH Privacy Board -- 415-255-3706



Cybersecurity: Phishing

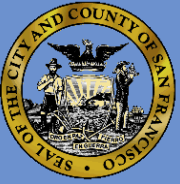
- **Phishing** is an attempt to obtain sensitive information such as usernames or passwords by masquerading as a trustworthy entity in an electronic communication
- **Phishing attempts** can also include delivering an attachment with malware or direct the user to a fraudulent website containing malicious code
- **Malicious links** can infect your computer and the network or take you to web pages designed to steal client 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.** Legitimate organizations will never ask for this information
- **When in doubt, “throw it out”** - delete emails and avoid web page links that look suspicious



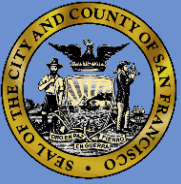


Resources

- See the OCPA Resources page for links to resources:

<https://www.sf.gov/departments/dph-office-compliance-and-privacy-affairs>

- Office of Compliance & Privacy Affairs (OCPA): compliance.privacy@sfdph.org or **(855) 729-6040**
- DPH IT Service Desk: **628-206-7378**
- 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.”**



Final Words

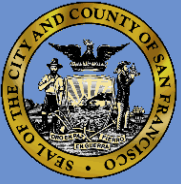
It's all about

➤ **Respect**

- **Respecting the privacy of the people we serve**

➤ **Trust**

- **They trust us to protect their privacy**

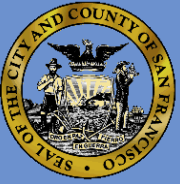


Thank You!

SFDPH values client privacy as an important part of our mission to provide quality healthcare with compassion and respect

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

*Thank
you!*



Next Steps

To receive credit for the annual Compliance and Privacy training you MUST:

1. Take and pass the Annual Compliance and Privacy Training Quiz (100% accuracy required)
2. Read and electronically sign the User Confidentiality, Security, and Electronic Signature Agreement
3. Read and electronically sign the Code of Conduct
4. Once steps 1-3 are completed, you will be awarded a Certificate of Completion