November 2021 Edition

San Francisco
Department of Public Health

PRIVACY PULSE

Safeguarding Electronic Protected Health Information (ePHI)

Encryption

Encrypt Your Electronic Devices:

- You need to encrypt ALL your electronic devices, whether CBO/UCSF/ DPH-owned, or your personal device. If you use a device for any CBO/UC/DPH purpose or to access any CBO/UC/DPH information, it must be encrypted.
- Remember: Encryption is the only safe method when Protected Health Information (PHI) or Personally Identifiable Information (PII)is involved. Click here for more information.

Secure Emailing

Encrypt Your Emails containing PHI:

- When sending PHI via DPH email, use your work email account only and activate encryption by using Secure in the subject line (Secure: for CSF)
- Do not put identifying information on the subject line.
- Do not send confidential information unless necessary. De-identify the information if possible. Send minimum necessary.
- Never use a personal email account, such as Yahoo, Gmail, or Hotmail, to send or receive emails containing PHI.

Text Messaging "SMS"

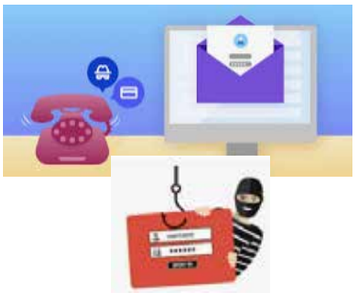
(Short Message Service)

NO Text Messaging of PHI allowed:

- SMS messages are not encrypted, cannot be recalled if sent to wrong person, and can be intercepted on public Wi-Fi networks.
- Sending patient data over SMS texting, iMessage, instant messaging, WhatsApp, or other texting apps is a **breach** of HIPAA regulations. These services are unsecure and non-compliant!

Phishing and Phone Scams

Phishing alarm button



What you should do if you receive a random email or call that asks for your private information:

- DO NOT reply or click on the link in the message. Within UCSF email, click on the Phishing Alarm button to report it. Or contact UCSF/DPH IT service desk immediately.
- If it's a phone message, hang up.
- DO NOT provide your personal or financial information.
  - Instead, if you believe the sender or caller to be legitimate organization, open a new internet browser session and type in the company's correct web address yourself. If you're concerned about your account, contact the organization mentioned in the email or call, using a telephone number you know to be genuine.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
- If you clicked on a phishing link or provided your credentials, change your password immediately and contact the IT Service Desk.
  - DPH (628) 206-7378/ UCSF (415) 514-4100
- DPH ONLY: If you receive an email and suspect it is a phishing email, forward to phishing@sfgov.org

Securing ePHI data

Securing CBO/UCSF/ DPH ePHI data, documents, and files:

- All data containing PHI should be save to UCSF/CBO/ DPH secured encrypted servers or UCSF/CBO/DPH sanctioned cloud storage or collaboration tools only (such as Office 365).
- DO NOT save PHI data to your computer / laptops' local drive or personal devices.
- DO NOT use non- sanctioned services such as Google Drive or other Cloud Server Services.

Report It!

Report every possible Breach of Protected Health Information (PHI):

- Email: compliance.privacy@sfdph.org
- Privacy Hotline: (855) 729-6040
- Refer to Breach Policy

The Privacy Office also provides consultation on all privacy-related questions. Please feel free to contact us.