# Safeguarding Electronic Protected Health Information

## Electronic Devices

It is the policy of SFGH to comply with state and federal laws governing the protection and confidentiality of PHI. This includes PHI in an electronic form.

- **Policy 8.17 Portable Devices, Removable Storage and Communication Device Security** must be followed. This policy protects SFGH data from unauthorized access and use, and to provide accountability for information use.
- **Encrypt** your electronic devices.
  - Check with IT support to ensure that your laptop, mobile devices, and flash drives are encrypted.
  - For additional information contact:
    - DPHIT at (415) 759-3577
    - UCSF-IT at (415) 514-4100
- Keep your device with you and in your possession at all times.
- If your electronic device is lost or stolen, you should notify your supervisor, site security and/or the police.

## Pagers

If you carry a pager and send or receive text pages, the following best practices should be followed:

- When constructing text pages, you should limit the amount of information to only what is necessary, such as first name or initials only.
- The goal is to minimize the risk of the patient actually being identified if the message reaches the wrong person.
- **Do NOT** text page confidential information, protected health information (such as diagnosis), or individually identifiable information.
- Text pages must be **deleted** on a daily basis or as soon as you finish reading them.
- If your pager is lost or stolen, please notify your supervisor immediately.

## Secure Emailing

Encrypt your emails containing PHI:

- When sending PHI via email, only use your work email account and activate secure email by using Secure: in the subject line
- **Do not** put identifying information on the subject line. Do not send confidential information unless absolutely necessary. De-identify the information if possible. Send only the minimum necessary to complete the task.
- Never use a personal email account, such as Yahoo, Gmail, or Hotmail, to send PHI
- Make sure the required confidentiality statement is on your email.

## Password Protection:

- **Never** share your password with anyone.
- Develop strong passwords, to increase the level of difficulty for someone to determine your password.
  - Use a minimum of 7-8 characters
  - Include numbers, letters (both upper and lower case), and special characters

## Report a Privacy Breach

Report every potential **Breach** of Protected Health Information (PHI):

- Privacy Officer: Maggie Rykowski (415) 206-4294
- Privacy Hotline: (855) 729-6040
- Email: Maggie.rykowski@sfdph.org or andreasun@ucsf.edu
- Policy: Reporting a privacy breach policy [#8.27]

The Privacy Office also provides consultation on all privacy related questions. If you have any questions, please feel free to contact us.