PRIVACY PULSE

San Francisco Department of Public Health

How to Prevent a Privacy Breach!

Unauthorized verbal disclosures (Verbal)

Gossiping / Sharing PHI:
- Please refrain from discussing patient information in public areas, such as the cafeteria, elevators, halls, waiting areas, or registration areas. Please remember that others may overhear what you say.
- Do not entertain gossip! Never share information about a patient with a friend or family.
- Other than a legitimate business reason (ex. direct patient care), there is no reason to discuss PHI with anyone. Plus, doing so comes with a hefty fine.
- Be sure you have the patient's permission before discussing confidential information in front of the patient's family members, friends, or caregivers.

Secure Emailing (Electronic)

Encrypt Your Emails containing PHI:
- When sending PHI via email, use your work email account only 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 necessary. De-identify the information if possible. Send minimum necessary.
- Never use a personal email account, such as Yahoo or Gmail to send or receive emails containing PHI.

Mishandling Paper PHI (Printed or written)

Handling printed and written PHI:
- Double-check all printed documents to make sure you are giving information to the correct patient.
- When handing documents, medications, or any other item containing PHI to a patient, **confirm the patient's identity** with at least two patient identifiers (ex. name, date of birth, MRN, phone number, home address, SSN) **before** handing anything to the patient. Also, then confirm that the correct name and identifiers match the information on each page or item you handing to them.
- Paper containing patient PHI should not be left unattended on copiers, printers, fax machines, or in common areas like break rooms or conference rooms.
- To dispose of paper containing PHI, place all pages in a secure shredding bin.
- **Do not take printed or written PHI off-site** unless authorized to do so (and on an encrypted, password-protected device). When traveling with PHI, always make sure it is securely with you.

Patient identification (Verification)

Proper identity checks at admission and registration:
- Ask the patient to confirm key identifiers, such as name, date of birth, social security number, phone number and address.
- Check the patient's identification (ID) against the appointment letter.
- Ensure that all the documentation, medical notes, and electronic systems used match the patient in front of you.
- Follow your area's patient identification policy

Proper identity checks during Specimen collecting and labeling:
- Specimens must be properly labeled at the time of collection, by using positive patient identification (full name, date of birth, and/or medical record number) prior to administering the patient's test and applying the label to the specimen.
- Specimen containers must be in the presence of your patient when labeling, to ensure it is the right patient and test.
- Double check the printed labels before placing it the specimen and make sure it matched the patient to the specimens collected.

Report It!

Report every Breach of Protected Health Information (PHI):

- Email: compliance.privacy@sfdph.org
- Privacy Hotline: (855) 729-6040
- Refer to DPH B1.1 Reporting of Unauthorized Access of PHI Policy

The Office of Compliance & Privacy Affairs (OCPA) also provides consultation on all privacy related questions. Please feel free to contact us.