Winter 2020 Edition

San Francisco
Department of Public Health

PRIVACY PULSE

IMPORTANT PRIVACY REMINDERS

Privacy Audits:

Stop. Think. Protect.

- You need to know that Audits are conducted at DPH on records of workforce members & high profile patients who are admitted to the hospital
- Audits of access in EPIC are conducted regularly. If you access records for non-business purposes, corrective and disciplinary actions may include loss of privileges, impact to your professional license and can lead up to termination of employment!
- Remember: Break-the-glass pop-up screen is to inform users that they are accessing a medical record that will trigger an audit alert to the Privacy Officer. Providing a comment when responding to the pop-up assists the Privacy Officer in determining if your access is authorized.

Password Security:

- NEVER share your confidential password with anyone!
- Always remember to log off your computer/laptop/work station when you are away from your desk.
- Always remember to log off or Tap out of EPIC when not in use. If someone else accesses a record while using your Log In, you will be responsible for that access.
- Use a Strong password is critical in keeping you and DPH secure. (Use Upper/lower case, numbers and symbols)

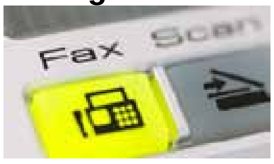
Social Media:

- Do not post digital images and messages containing protected health information (PHI) without written authorization from the patient and written approval from ZSFG Administration
- Any known or suspected incident involving use or disclosures of patient information through social networking are to be reported to the Office of Compliance & Privacy Affairs
- Policy for social networking and other web-based communications [#8.29] must be followed!

Handing Patient PHI Documents:

- Double check the documents and ensure you take only the patient information that pertains to the person when removing the documents from the printer.
- Check all pages of the documents to ensure that the information relates to the patient that you are giving it to and all pages are printed correctly.
- Ask the patient to confirm their name and date of birth to verify that you have the right match **before** you give them the documents with PHI.

Faxing:



- Always verify the recipient's fax number before transmitting
- Always use a cover sheet with a confidentiality statement
- Always send only the minimum necessary!
- Reference Policy for secure transmission of protected health information (PHI) [# 8.14]

Emailing:

- 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 any PHI or identifying information on the subject line.
- Do not send confidential information unless absolutely necessary. De-identify the information if possible
- Never use a personal email account, such as yahoo, Gmail, or Hotmail, when sending PHI

Report a Privacy Breach:

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

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

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