Do you think HIPAA is no BIG deal?
The U.S. Department of Health and Human Services for Civil rights (OCR) is responsible for enforcing the privacy and security rules. At DPH, we are required to comply. Below are example of penalties and fines that OCR has issued to their violators. Be aware of your actions to reduce Privacy violations. ***** STOP, THINK, PROTECT!******

Penalties and fines involving Paper PHI

PHI must be protected when it travels

- A clinic schedule and encounter forms containing PHI were left on a Boston subway by a hospital employee.
- A $1 Million fine was paid by the hospital.

You should never take PHI offsite without a specific business need. If you need to, never leave records unattended and keep them with you at all times.

NOTHING with PHI should ever go in the trash!!!

- CVS paid $2.25 Million and Rite Aid $1 Million in fines for throwing away prescription bottles and paper prescriptions in the dumpsters.

All PHI must be properly disposed and paper PHI must be properly shredded or placed in a secure shred bin.

Requested PHI went elsewhere

- Patient requested information to be sent to a personal post office box. Provider instead faxed PHI to his employer, including HIV status, Mental health history, and sensitive diagnoses.
- $387,000 fine paid by the hospital.

Proper release of PHI authorization must be obtained from the patient first. Authorized Release instructions on the patient's form must be followed.

Other Facts: Any paper PHI that is lost or gets into the hands of the wrong person, such as handing a lab requisition to the wrong patient could be a breach that must be reported to CDPH, the patient involved AND the Office for Civil Rights. We are subject to fines and penalties for any late reporting. Double-check the documents before handing them to the patient.

Penalties and fines involving unauthorized disclosures

Think before you share PHI verbally!

- One employee shared PHI of 1 patient with a mutual acquaintance
- Outcomes: $1.4 Million verdict for walgreens in a civil suit.
- OCR action and federal fines still possible!

Avoid sharing PHI with anyone who does not need to know. Do not discuss patient medical information in front of the patient's visitor, unless authorized by the patient.

Penalties and fines involving unauthorized accesses

Snooping out of curiosity

- UCLA paid $865,000 in fines when an audit showed employees had accessed patient records unrelated to their job!
- Multiple employees were terminated.

Audits of access are conducted regularly on the electronic medical record. If you access records for non-business purposes, corrective and disciplinary actions may include loss of privileges, impact to your professional license and termination of employment.

Report a Privacy Breach:

<table>
<thead>
<tr>
<th>Report every potential Breach of Protected Health Information (PHI):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Hotline: (855) 729-6040</td>
</tr>
<tr>
<td>Email: <a href="mailto:compliance.privacy@sfdph.org">compliance.privacy@sfdph.org</a></td>
</tr>
<tr>
<td>Refer to Policy# B1.1 Reporting of Unauthorized Access of PHI</td>
</tr>
</tbody>
</table>

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