# COMPLIANCE AND PRIVACY MATTERS

## DPH Office of Compliance and Privacy Affairs – June 2024

## HIPAA Compliance – What is a HIPAA Breach?


What is a HIPAA breach?

A “breach” as defined by the Health Insurance Portability and Accountability Act (HIPAA) is an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information (PHI).

In other words, a breach occurs when PHI is viewed or disclosed with a person or entity who does not have the authority to see it.

What types of incidents would constitute a breach?

- Viewing a patient record that you have no work-related reason to view, including your own.
- Disclosing patient information to someone not involved in the patient’s care, including other co-workers.
- Informing a patient’s family member or friend about their care without getting the patient’s permission.
- Losing PHI that cannot be recovered, including in electronic devices.
- Giving paperwork about a patient to the wrong person, for example: sending a patient home with someone else’s after visit summary.

What to do if you think you may have compromised PHI?

- REPORT IT IMMEDIATLEY! Even if you are not sure if the incident is a breach, you must report it. OCPA will determine if the incident is a reportable breach.
- Delayed reporting can increase fines and consequences for both DPH and individual employees.

**Remember:** Not everyone has a job-related reason to see individual patients’ PHI. Think about who you are disclosing information to, and if they have a reason to know it.

**OCPA COMPLIANCE AND PRIVACY HOTLINE**
**855.729.6040 – compliance.privacy@sfdph.org**

**SAN FRANCISCO DEPARTMENT OF PUBLIC HEALTH**
**Office of Compliance and Privacy Affairs**