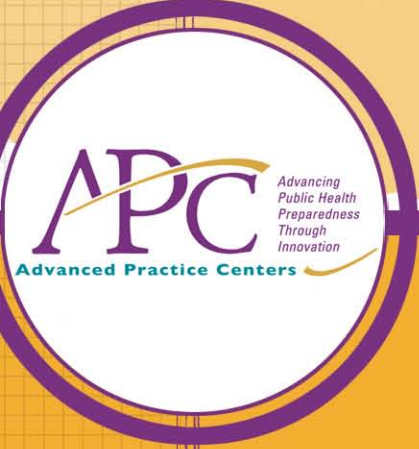




**Public Health**  
Prevent. Promote. Protect.





# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT



This information is required to work with and around patients. Please read. Contact [Jeff.Cappe@phd3.idaho.gov](mailto:Jeff.Cappe@phd3.idaho.gov) if questions.

# Learning Objectives



- By the end of this section the participant should be able to:
  - Define Health Insurance Portability and Accountability Act (HIPAA)
  - Identify protected and unprotected health information
  - Describe how HIPAA applies in a disaster situation

# What is HIPAA?

- Health Insurance Portability and Accountability Act (HIPAA)
  - Public Law 104-191: Signed August 21, 1996
- A federal law designed to:
  - Give patients control over all Protected Health Information (PHI) that might be shared between health care providers & other covered entities
  - Ensure confidentiality of PHI
- Standards set by HIPAA are minimal, therefore state and local lawmakers may enforce strict guidelines to protect a person's private health information

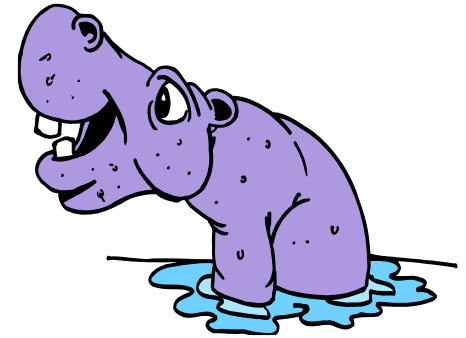
# What is protected?



HIPAA protects communications between patients , their healthcare provider, and anyone working in the organization from housekeeper to CEO that are:

- verbal
- written
- electronic

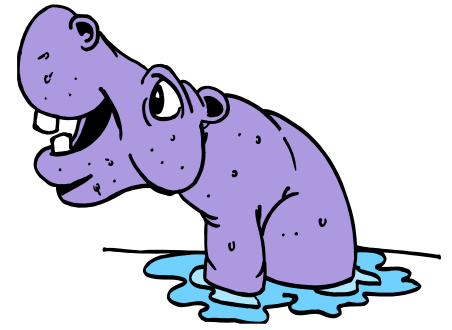
# What Is Protected Health Information (PHI)



## Health Information:

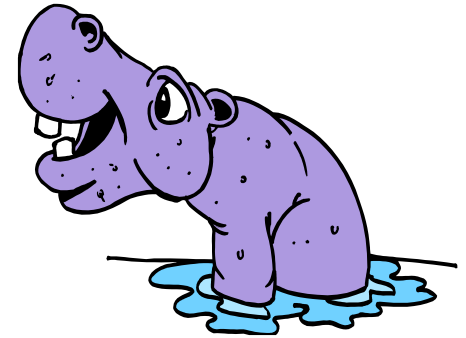
any oral or recorded information relating to the past, present or future physical or mental health of an individual, health care provided to the individual, or the payment for health care.

# What is Protected Health Information



Information about a patient created or received by a hospital, clinic, emergency provider, or public health:  
is protected under the HIPAA privacy rule.

# What is Protected Health Information



## Individual Identifiers:

information that identifies or can be used, alone or in combination with other information, to identify the individual (e.g., name, address, SSN, anything found in a patient medical note, directive, or record, etc).

# What Healthcare Entities Are Covered?

- Health Departments
- Health Plans – individual or group health insurance companies
- Health Care Clearinghouses – billing services or providers
- A health care worker who transmits any health information in electronic form – hospitals, clinics, doctors, nurses, and EMS

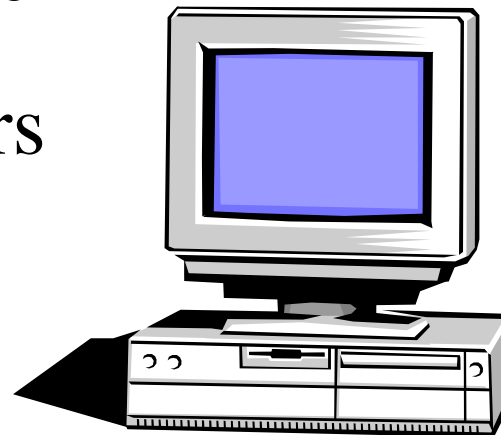
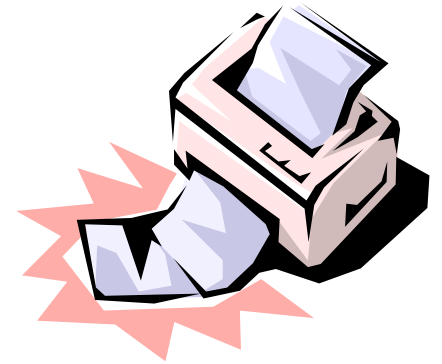
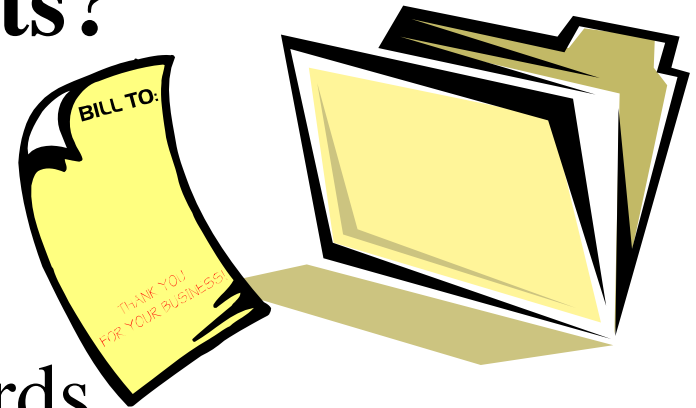
# Types of Individual Identifiers

- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locations (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable data
- Any other unique identifying number, characteristic, or code

# Where are the places **Protected Health Information** exists?

**PHI** may be found:

- in medical and billing records
- at the fax machine
- on your computers

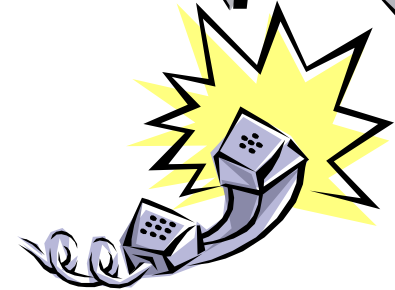


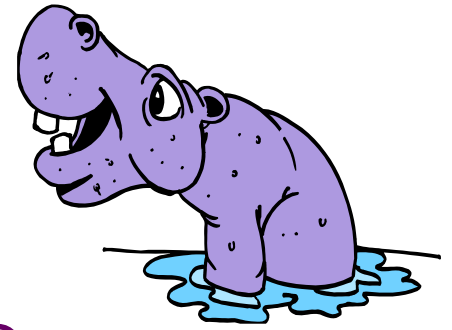
# Where are the places **PHI** exists?

**PHI** may be found:

- in your files;
- on your desk;
- in telephone conversations or overheard conversations

**Look around, you may be surprised at all of the places **PHI** exists in our environment.**





# The HIPPA Privacy Rule

Rule that defines and limits how a covered entity shares individual identifiable health information

## Commitment to Privacy



- **Every organization has a commitment to protect patient privacy. (confidentiality)**
- **Before HIPAA, no federal framework existed to protect patient information from being exploited for personal gain.**
- **Under HIPAA, organizations and individuals will be punished for violating privacy clauses.**

# Exceptions to Privacy Rule

- HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule.
  - For example, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information.

# HIPAA in a Disaster

- The HIPAA Privacy Rule allows patient information to be shared to assist in disaster relief efforts, and to assist patients in receiving the care they need.

# HIPAA Disaster Policy Summary

- The ways in which patient information can be shared by providers and health plans covered by the HIPAA privacy rule are:
  - About Treatment
  - Notification
  - Imminent Danger
  - Facility Directory

# Treatment

- Health care providers can share patient information as necessary to provide treatment.
- Treatment includes
  - sharing information with other providers (including hospitals and clinics)
  - referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
  - coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).
- Providers can also share patient information to the extent necessary to seek payment for these health care services.

# Notification

- Health care providers can share patient information as necessary to identify, locate and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.
  - The health care provider should get verbal permission from individuals, when possible; but, if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgment, doing so is in the patient's best interest.
    - Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify or otherwise notify family members and others as to the location and general condition of their loved ones.

# Notification, cont'd

- In addition, when a health care provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.

# Imminent Danger

- Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public
- Sharing of PHI should be consistent with applicable law and the provider's standards of ethical conduct.

# Facility Directory

- Health care facilities maintaining a directory of patients can tell people who to call or ask about individuals whether the individual is...
  - at the facility
  - His/her location in the facility, and
  - His/her general condition.

# Questions

- Contact [Jeff.Cappe@phd3.idaho.gov](mailto:Jeff.Cappe@phd3.idaho.gov)
- Or the Idaho Hospital Association