



# **HIPAA: Beyond the Basics**

---

## **Security of Client Information**



# What is HIPAA?

Healthcare Insurance Portability and  
Accountability Act of 1996

- Became effective on 04/14/2003
- Electronic standards to improve efficiency & effectiveness of healthcare.
- Protections for security & privacy of individually identifiable health information.



## Why is this important for volunteers?

- All providers of health care, regardless of whether or not they are employed or volunteering, must comply with HIPAA statutes
- The agencies with which we volunteer (public health, hospitals, clinics, etc) are all responsible for complying with HIPAA regulations



## Who is Affected?

- Covers virtually anyone who provides healthcare services to consumers and engages in any electronic transaction.

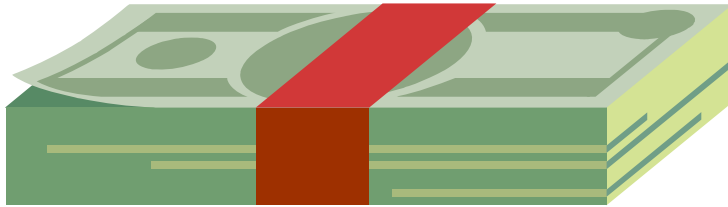


Includes all of us involved in the FC&C MRC.



# Why Be HIPAA Compliant?

- **It's a law!** Civil penalties up to \$250,000 or more per person.



- It's good risk management. No sense in putting the agencies we work with at risk for bad publicity or lawsuit.

- It's good business to protect client health information.





# Your Responsibility

- Safeguard **Protected Health Information (PHI)** regardless of its format (hardcopy, electronic, verbal, etc.)
- Treat PHI as strictly confidential- even among other volunteers.
- Prevent PHI from loss, tampering, alteration, destruction, unauthorized access or inadvertent disclosure.



# What is PHI?

**Any client information, verbal or written, that is:**

- **Related to past, present, or future health of client.**
- **Regarding client's caretakers, family members and friends.**
- **Created or received by you or the agency with which you are volunteering.**
- **Related to healthcare received.**
- **Shared to obtain payment.**





## Individually Identifiable Health Information is:

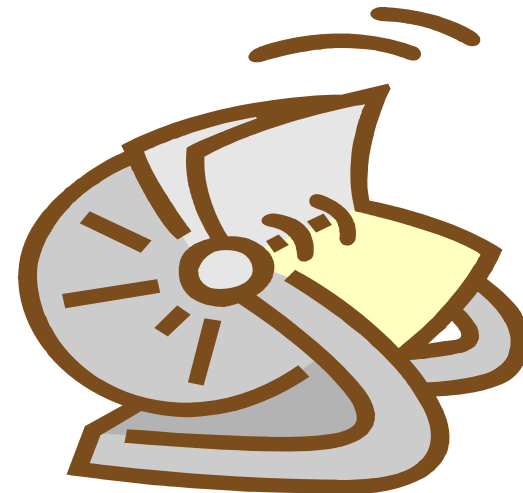
**Any information that identifies the individual.**

**Information that could be used to identify the individual.**



## Examples of Individual Information (PHI)

- Name
- Geographic subdivision (zip codes, etc.)
- Date of birth
- Telephone or fax numbers, e-mail, web address
- Social security number
- Medical record number
- Health plan number





## More examples of PHI



- Account number
- Certificate/license number
- Vehicle identifier
- Device identifier
- Biometric identifier (fingerprints, etc.)
- Photographic image
- Any other unique characteristic or code





# Forms You May Use

- **Disclosure Log**

- **Privacy Notice and Acknowledgement**

**Authorization to  
Release  
Information**

**Consent for  
Pictures and  
Statements**



# Privacy Notice

**Describes how medical information may be:**

- Used
- Disclosed
- Access by client
- Limited by client





## Privacy Notice May Be:

- Given to client during a disaster situation
  - Distribute **most current version available** in English, Spanish, or Somali.
- Reviewed by client.



**NOTE:** whether or not the privacy notice is distributed, PHI remains confidential, even in an emergency!



## Privacy Notice Must Be:

- Acknowledged by client's signature on Acknowledgement of Receipt form.

- Posted in all program areas.



## Permitted Uses & Disclosures of PHI



- To carry out treatment, payment and health care operations.
- With a valid **authorization**.



## Disclosures Permitted Without Required Authorization:

- For public health activities to conduct public health surveillance or investigations.
- Health oversight activities, such as those from the healthcare system or government benefit programs where health information is relevant to eligibility.





## Other Disclosures Permitted Without Authorization:

- Judicial & administrative proceedings.
- Law enforcement purposes.
- Victims of abuse, neglect, domestic violence.
- Death (medical examiners/funeral homes).
- Organ & tissue donation.
- Medical research (de-identified info only).
- Serious threats to health or safety.
- Specialized government functions.
- Correctional institutions.



# Client Rights

- Limit our partner agency's use of their PHI.
- Define how they will be contacted.
- Review their PHI.
- Obtain copies of their PHI.
- Request to change their PHI.
- Receive accounting of disclosures of PHI.
- File a complaint if breach of HIPAA rules is suspected.





## If a Client Files a Complaint:

1. Ask client/personal representative to complete HIPAA Complaint Form.
2. Assist in completing form if needed.
3. Receive completed form.
4. Route form to Privacy Office and supervisor of work area named in complaint.





## When a Client Files a Complaint:

### **Supervisors:**

- Investigate all complaints.
- Report findings to Privacy Officer.

### **Privacy Officer at partner agency:**

- Responds to client/personal representative with investigation results.



## Privacy Notice and Acknowledgement

**Privacy Notice  
is given to  
client.**

**Acknowledgement  
is placed in  
client's record.**



# Authorization Form

**Authorization is required for any disclosure unless required by law.**

**It must:**

- Specify information to be disclosed.
- Identify program or agency making disclosure.
- Be signed and dated by client or personal representative.
- **NOTE:** If client can only make an “X” or other marking, an adult witness must note on authorization that this is the client’s mark.



## Authorization Valid ONLY if it Contains:

- Client's name
- Client's date of birth or social security number
- Agency or person to whom PHI will be released
- Agency or person releasing PHI
- Type of PHI requested





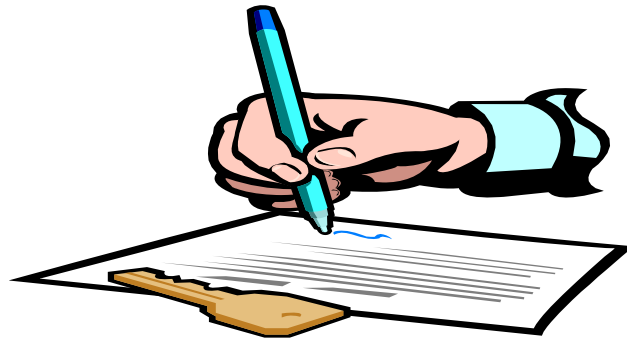
## Authorization Valid ONLY if it Contains:

- Purpose or need for PHI.
- Revocation statement that says client can cancel authorization at any time.
- Re-disclosure statement that says recipient cannot further release this information without written consent of client.



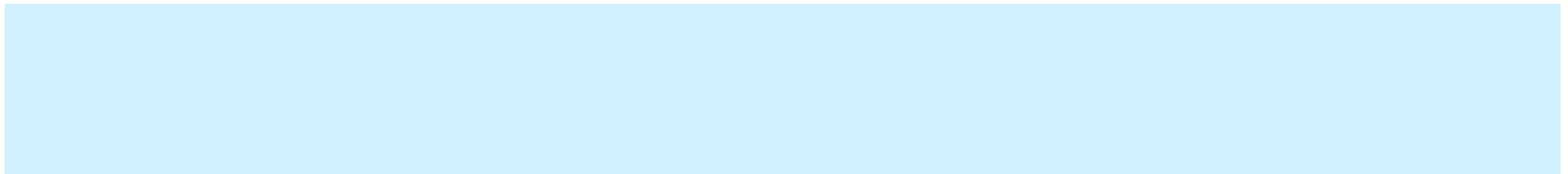
## Authorization Valid ONLY if it Contains:

- Expiration date, event or condition upon which authorization expires.
- Signature of client/personal representative.
- Signature of adult witness.
- Date authorization was signed.





# Authorization NOT Considered Valid If:





## Additional Points About Authorizations

- Release only the **minimum** amount of PHI necessary to accomplish the purpose of the request.

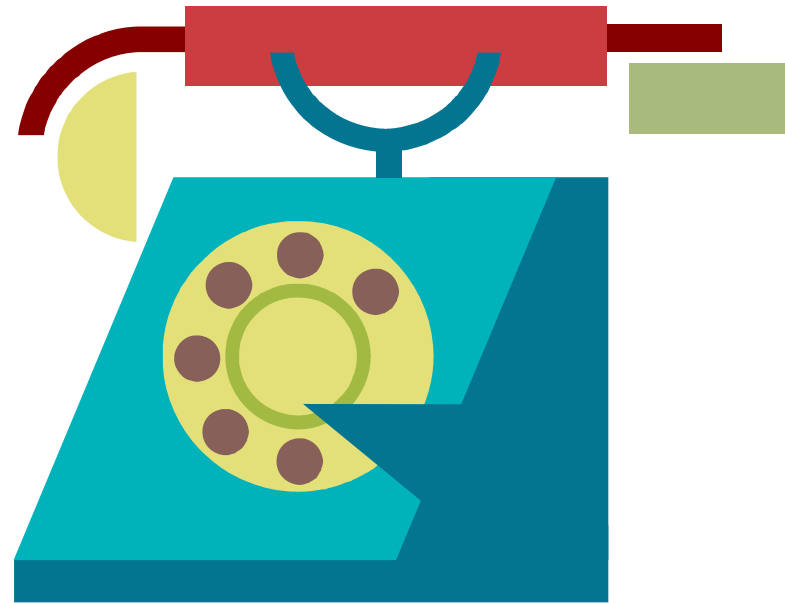


- Send copy of authorization to client after sending copies of PHI to requestor.



# Telephone requests for PHI

Some programs cannot legally release PHI by phone. Ask your supervisor if this is something that should be performed.





## Request to Inspect and/or Obtain PHI

This will most likely differ depending on the agency with which you are responding. Talk to your supervisor.

- Client/personal representative must sign HIPAA-compliant authorization.
- Client/personal representative may have access except for:
  - Psychotherapy notes.
  - Information compiled for used in civil, criminal or administrative proceedings.
  - Information protected by Clinical Lab Improvements Amendments of 1988 (CLIA).



# Subpoenas and Court Orders

Upon receipt of subpoena or court order:

- Route to supervisor as soon as possible.
- Program manager/designee will:
  - Fax subpoena/court order to City Attorney for determination of validity & for further instructions.
  - Contact issuer of subpoena/court order to ask whether certified copies of PHI may be sent in lieu of court appearance by agency employee.

**NOTE:** Threats and intimidation from requestor must be reported to your supervisor ASAP!!!



# Faxing PHI



- If fax is sent to wrong recipient, request that fax be destroyed immediately and inform supervisor.



- Verify recipient of fax and confirm fax number before sending.

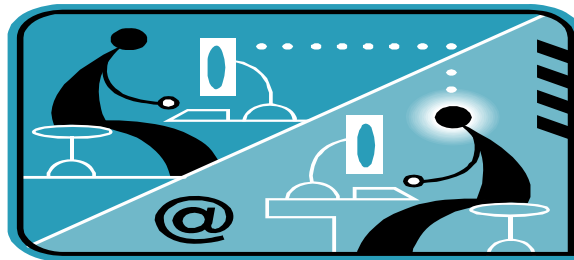


- Retain fax cover sheet in client's record.



## E-mail

- PHI must **NOT** be e-mailed outside of agency's e-mail system.



- If PHI is e-mailed **within** agency's system, it must contain Confidentiality Notice ("This e-mail, including any attachments...").



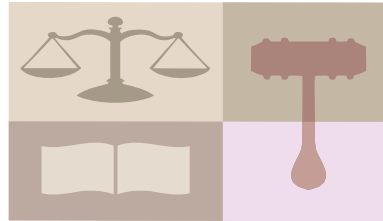
# Accounting of Disclosures

- Client has the right to a written accounting of disclosures made in the last 6 years.
- Information required:
  - Date of disclosure.
  - Name of entity to whom disclosure was made.
  - Description of information disclosed.
  - Statement regarding purpose of disclosure.



## Additional Considerations Regarding HIPAA

- HIPAA establishes the floor, not the ceiling.
- More stringent state and federal laws must take precedence.



- If current law is silent, HIPAA becomes the de facto standard.
- As a rule, do not talk about PHI with other volunteers or even with your family.



# Employee Responsibilities for Security of Client Information

Employees using **portable computing devices and/or removable storage component devices**, such as diskettes, CD's, DVD's, & flash memory cards must:

- Protect these items from unauthorized access.
- Utilize physical security measures.





# Physical Security Measures

Devices must not be left unattended without using:

Cable  
Locks

Restricted access  
environments.

Lockable  
cabinets.



# Physical Security Measures

- As much as possible, devices and PHI papers must remain under employee's visual control.
- If impossible to do this, necessary safeguards must be used to protect devices.
- Avoid unauthorized viewing of PHI in public or common areas.



## Removal of PHI from the Premises

**Volunteers must never remove PHI** stored on any device or otherwise maintained in any manner from the responding agency's location, whether it be a temporary location or the main clinic.



# E-mailing PHI

As mentioned in a previous slide, PHI will **NOT** be e-mailed to anyone outside the agency's e-mail system.





## Proof of Training

Please don't forget to complete the post-training questions on the intranet site. This serves as proof that you have undergone the training.

**Thank you!**