

HIPAA Privacy and Security in Local Government

CLHO Mentorship Program

12-14

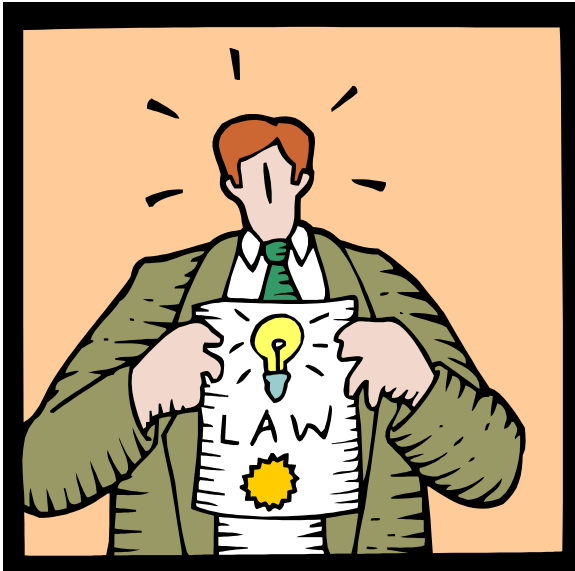
TRAINING GOALS



- ▶ Understand the purpose of HIPAA
- ▶ Understand “protected health information”
- ▶ Understand the rules for use and disclosure of protected health information
- ▶ Know where to find the County privacy policies and procedures
- ▶ Understand that the County share protected health information with its business associates
- ▶ Know who the County Privacy Complaint Officer is?

What Is Health Insurance Portability and Accountability Act?

HIPAA is a Federal law enacted to:



- ✿ **STANDARDS** to protect the privacy and security of individuals Protected Health Information (PHI)
- ✿ **STANDARDS** for the physical and electronic security of PHI
- ✿ **ENSURE** security of health care info (paper, written, electronic)
- ✿ **SIMPLIFY** billing and other transactions
- ✿ **EXTEND** the rights of individuals over the use of their protected health information

OVERVIEW OF HIPAA

- ▶ Health Insurance Portability and Accountability Act of 1996
 - Into effect April 2001
 - Compliance required by April 2003
 - Kennedy/Kassanbaum Act



What Is Health Insurance Portability and Accountability Act?

- ▶ Ensure that business associates protect our patients' information
- ▶ Mandates training for workforce members on standards and policies
- ▶ Designate an agency Privacy Officer
- ▶ Establish a Complaint Procedure



WHAT DOES THIS HAVE TO DO WITH ME?

vital statistics

County records

Public health services

medical records

AIDS/HIV

tuberculosis

preparedness

Contracted client services

public health reporting

corrections

Employee health records

- ▶ Client records
- ▶ Disease reporting
- ▶ Registries
- ▶ Identifiable client information
- ▶ Personnel Records - Medical

HIPAA rules apply to a significant part of the county!

Do the HIPAA laws apply to **you**?

The Health Insurance Portability & Accountability Act (HIPAA) requires that Counties train all members of its workforce about the County's HIPAA Policies and specific procedures required by HIPAA that may affect the work you do.



WHY?



- ▶ Highly public breaches of privacy
- ▶ Increasing public concern around privacy
- ▶ Ten people fired over Octo-Mom case
- ▶ Release of celebrity files...
- ▶ Hopefully not yours!!!!
- ▶ More than 25 cents of every health-care dollar is spent on administration
- ▶ Hundreds of different billing forms
- ▶ National changes requested by providers

HIPAA: At the Office



- ▶ If you have a co-worker, HIPAA will come into play!
- ▶ Is anyone sick in your office?
- ▶ Did you overhear a conversation between a co-worker and the supervisor?
- ▶ Was there a workers comp injury?
- ▶ Remember: when it comes to HIPAA protected information, NOTHING IS PUBLIC KNOWLEDGE!

ADMINISTRATIVE SIMPLIFICATION

- ▶ **Privacy Rules**
- ▶ **Security Rules**
- ▶ Transactions and Code Set Standard
- ▶ Identifier Standards
 - Employer Identifier Standard
 - National Provider Identifier Standard (NPI)



What Information Must We Protect?

- ▶ We must protect an individual's personal and health information that...
 - Is created, received, or maintained by an organization and relates to past, present, or future
 - Is written, spoken, or electronic
 - And, includes at least one of the 18 personal identifiers in association with health information



Health Information with identifiers = Protected Health Information (PHI)

To the Individual, it's all Confidential Information

- ▶ *Personal* Information
- ▶ *Financial* Information
- ▶ *Medical* Information
- ▶ Written, Spoken, Electronic *PHI*

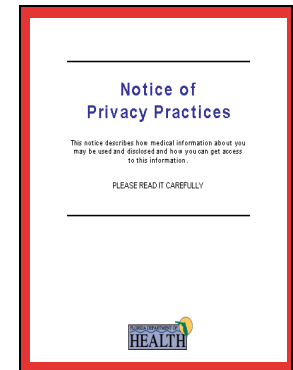


Protected Health Information (PHI): 18 Identifiers defined by HIPAA

- ✓ Name
- ✓ Postal address
- ✓ All elements of dates except year
- ✓ Telephone number
- ✓ Fax number
- ✓ Email address
- ✓ URL address
- ✓ IP address
- ✓ Account numbers
- ✓ License numbers
- ✓ Social security number
- ✓ Medical record number
- ✓ Health plan beneficiary #
- ✓ Device identifiers and their serial numbers
- ✓ Vehicle identifiers and serial number
- ✓ Biometric identifiers (finger and voice prints)
- ✓ Full face photos and other comparable images
- ✓ Any other unique identifying number, code, or characteristic.

In Order for the County to Use or Disclose **PHI**

- The County must give each patient a **Notice of Privacy Practices** that:
 - Describes how the County may use and disclose the patient's protected health information (PHI) and
 - Advises the patient of his/her privacy rights
- The County must attempt to obtain a patient's signature acknowledging receipt of the Notice, EXCEPT in emergency situations. If a signature is not obtained, the County must document the reason it was not.



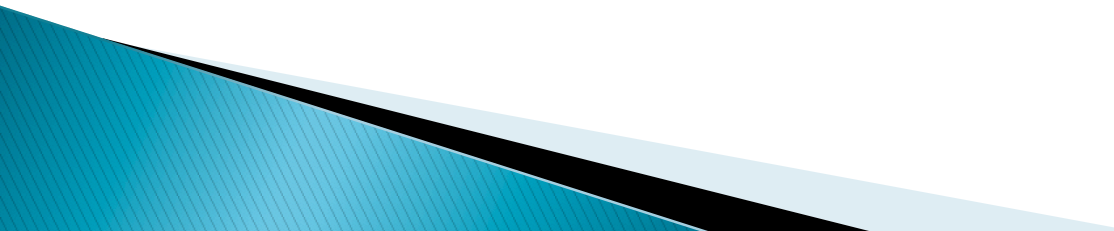
But, for purposes other than treatment, payment, operations...



Unless required or permitted by law the County must obtain written authorization from the individual to use, disclose or access personal information:

- **Individual Authorization** - allows for County to disclose information for other purposes (§164.508)
- **Minimum Necessary** applies to all uses and disclosures for payment and all healthcare operations (§164.502(b), (§164.514(d))

Clients Have The Right To:

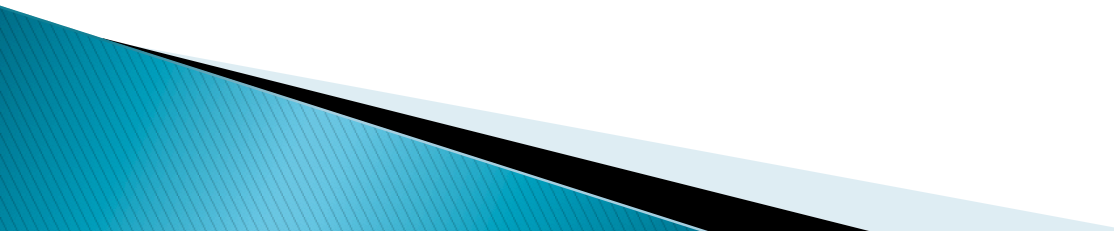
- ▶ Receive a written notice of the privacy practices
 - ▶ Require their authorization for the release of information
 - ▶ Request restrictions on the use of their PHI
 - ▶ Inspect and copy their PHI – as documented by the Department
 - ▶ Request that improper uses are corrected
 - ▶ Obtain a report of disclosures of their PHI
 - ▶ File a grievance or complaint.
- 

USES AND DISCLOSURES



- ▶ **Rule:** in general, individually identifiable health information is confidential and not to be disclosed.
 - **Casual conversation**, in or out of the workplace, regarding patient's or employee's physical or mental condition or treatment.
 - **For example**, if an employee calls in sick, you may report that the employee is home ill, but you may not report what the illness is....It is better to say employee is out today.

EXCEPTIONS

- ▶ PHI may be disclosed for Public Policy:
 - Reporting of Disease
 - Victims of abuse, neglect, domestic violence
 - Health oversight activities
 - Judicial and administrative proceedings
 - Law enforcement purposes
 - Serious threat to health or safety
 - Birth and death
 - Research and statistical purposes
- 

USE REASONABLE SAFEGUARDS

- ▶ **Reasonable Safeguards** are the actions the Departments take to ensure that protected health information remains private.
- ▶ When there is incidental use or disclosure of health information, use these *reasonable safeguards*:
 - Access is limited
 - Authorization is obtained prior to sharing (when applicable)
 - Client information is physically secure



REASONABLE SAFEGUARD EXAMPLES

The Security Policy specifies precautions that should be taken to assure information privacy and security

- ▶ Speak quietly when discussing a client's condition with family members or others
- ▶ Avoid using client names in elevators and hallways
- ▶ Secure documents in locked offices and cabinets
- ▶ Use passwords and other security measures on computers, security screens
- ▶ Written policies and procedures
- ▶ Shredders



INCIDENTAL DISCLOSURES AND HIPAA

- ▶ “Incidental”: a use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a by-product of an otherwise permitted use or disclosure. (§164.502(c)(1)(iii))
- ▶ These are allowable as long as *reasonable safeguards* are taken and the sharing of protected health information is *limited to the minimum necessary to do the job*.



WE NEED TO **PROTECT** THE ENTIRE LIFECYCLE OF INFORMATION - SECURITY

- ▶ Intake/creation of PHI
- ▶ Storage of PHI
- ▶ Destruction of PHI
- ▶ For any format of PHI



INFORMATION CAN BE **LOST**...

Physically lost or stolen...

Paper copies, films, tapes, devices
Lost anywhere at anytime-streets, restrooms,
coffee shops, left on top of car
when driving away from business ...

Or

Misdirected to outside world...

Mislabeled mail, wrong fax number, wrong
phone number
Wrong email address, misplaced on CC
internet
Not using secured email
Verbal release of information without patient
approval



ELECTRONIC INFORMATION CAN ALSO BE LOST OR STOLEN

- ▶ Lost/stolen laptops, PDAs, cell phones
- ▶ Lost/stolen zip disks, CDs, flash drives
- ▶ Unprotected systems were hacked
- ▶ Email sent to the wrong address or wrong person (faxes have same issues)
- ▶ User not logged off of system



Good Computing Practices

1. Passwords
 2. Lock Your Screen
 3. Workstation Security
 4. Portable Device
 5. Data Management
 6. Anti Virus
 7. Computer Security
 8. Email
 9. Safe Internet Use
 10. Reporting Security Incidents / Breach
- 

REPORTING SECURITY INCIDENTS/ BREACH

1. Immediately report anything unusual, suspected security incidents, or breaches to your supervisor.
2. This also goes for loss/theft of PHI in hardcopy format (paper, films etc).



CROOK COUNTY COMPLIANCE

- ▶ The Act required covered entities, including Counties to adopt policies and procedures for the protection of PHI
- ▶ The Act requires covered entities to conduct training sessions on a regular basis
- ▶ Who is Your Designated Privacy Officer?



COMPLAINT /GRIEVANCE PROCEDURE



**Client believes rights under HIPAA
may have been violated**



**Patient files a written complaint with local
Privacy Officer**



**Local Privacy Officer coordinates investigation
with DOH Privacy Complaint Officer
(Inspector General)**



**If issue not resolved to patient satisfaction, he or
she can file a complaint or grievance with the
Department of Health and Human Services Office of
Civil Rights**

HIPAA **Violations** Can Carry Penalties--

▶ Criminal Penalties

- \$50,000 - \$250,000 fines
- Jail Terms up to 10 years

▶ Civil Monetary Penalties

- \$100 - \$25,000/yr fines
- more \$ if multiple year violations



HIPAA **Violations** Can Carry Penalties--

- ▶ Fines & Penalties – Violation of State Law
- ▶ County corrective & disciplinary action
 - Up to & including loss of privileges and job loss
 - There can be no retaliation against someone reporting
 - Supervisor must make sure employees understand rules.



CROOK COUNTY HIPAA POLICIES AND PROCEDURES

- ◎ The HIPAA Policies and Procedures are in each County
- ◎ “The intent of this policy is to outline general guidelines and expectations for the necessary collection, use, and disclosure of confidential information about individuals in order to provide services and benefits to individuals, while maintaining reasonable safeguards to protect the privacy of their information.”



COVERED ENTITY



- ▶ Any person or business that either creates or receives PHI is a covered entity.
- ▶ The County is considered a “hybrid” covered entity due to the fact that all departments either create or receive PHI.
- ▶ If your department creates or receives PHI, the HIPAA applies to you.

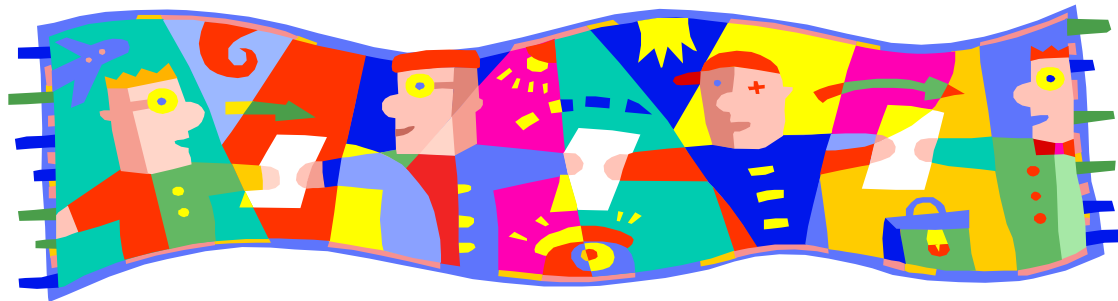
WHY IS PROTECTING PRIVACY AND SECURITY IMPORTANT?

- ▶ We all want our privacy protected!
- ▶ It's the right thing to do!
- ▶ It's the law and it's county policy!



HIPAA INFORMATION RESOURCES

- ▶ Your County HIPAA Policy
- ▶ US Dept. Of Health and Human Services:
<http://www.hhs.gov/ocr/hipaa/>





**The End
Questions?**