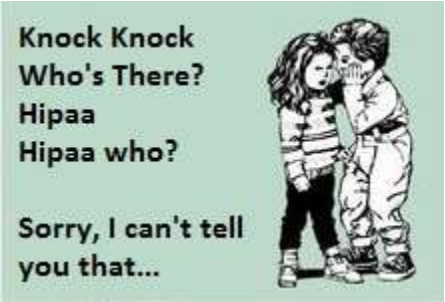
HIPAA PRIVACY AND SECURITY WORKBOOK

Chester County
HIPAA Hybrid Covered Entity
February 13, 2020

Table of Contents

Section I - Introduction

What is HIPAA?



HIPAA stands for the

Health

Insurance

Portability and

Accountability

Act of 1996.

HIPAA is designed to protect insurance coverage for workers and their families when they change or lose their jobs (portability) and to regulate the integrity, confidentiality and availability of personal health information (accountability). Most of the provisions of HIPAA were fully implemented by 2005.

Prior to HIPAA, there were no national standards on the privacy and security of individually identifiable personal health information. HIPAA established rules about individual access to and control of one's own health records and new standards for the privacy, security, and sharing of health care information. These uniform, national standards for paper and electronic transactions involved the creation of unique health identifiers, uniform code sets for health care transactions, electronic signatures, and security policies and procedures. The HIPAA Privacy Rules were effective April, 2003, while the Security Rules were implemented in April, 2005.

Who is subject to the HIPAA Rules?

Three types of organizations are subject to the rules: health care plans, health care providers, and health care clearinghouses. Anyone who works for, or in some cases with, these types of organizations must comply with HIPAA rules.

The term "covered entity" describes those organizations subject to HIPAA provisions. Organizations with a sub-group of departments performing qualifying activities are "hybrid" covered entities, so that only the departments in the hybrid entity

are required to comply with HIPAA. **Chester County qualifies as a hybrid covered entity because not all departments perform health care transactions**.

Departments designated in the hybrid covered entity are:

Aging	Controllers
Children, Youth and Families	Computer & Information Services
Drug & Alcohol	Dept. of Community Development
Managed Behavioral Healthcare	Archives and Records
Mental Health /Intellectual & Developmental Disabilities	
Health Department	Youth Center
Commissioners	Pocopson Home

Employees in these departments must understand and follow HIPAA rules, including:

- Persons involved in treatment including *but not limited* to doctors, nurses, patient educators, therapists, medical students, interns, case workers;
- Persons involved in billing activities including but not limited to accounts payable and accounts receivable personnel, billing clerks, collection representatives, and those involved in verifying health insurance information;
- Persons involved in business operations including but not limited to quality improvement staff, risk managers, auditors, analysts and medical records staff.

Business Associates

Covered entities sometimes contract with other organizations, or business associates, to provide administrative or operational services such as benefit management, claims processing, data analysis, or legal services. To allow sharing of protected health information, HIPAA requires covered entities to have written assurances from business associates that they will use protected information for intended purposes only, and will safeguard the information from misuse.

HIPAA and State Laws

HIPAA provides minimum protections for personal health information where none existed previously. In states where **existing state law** is more stringent, **state law supersedes HIPAA**. If it would be impossible for a covered entity to comply with both state law and HIPAA, or if the state law is an obstacle to accomplishing the objectives of HIPAA, then HIPAA preempts state law. Department Heads provide information on specific department functions and HIPAA compliance.

Section II – HIPAA Privacy Rules

Overview

Imagine how you would feel if a co-worker reviewed your records, learned about your protection from abuse order, and then shared this information with co-workers or other people. Imagine how you would feel being a patient at a county health clinic where your personal health information was discussed openly in front of other patients or staff. Imagine how you would feel if the mortgage company where you have a home loan application could get your personal health information from your health insurance company.

The HIPAA Privacy Rules govern the use and disclosure of protected personal health information. They specify what data is protected, what uses require prior authorization, and client privacy and access rights. The rules identify who is responsible to create and maintain the protection safeguards, and hold *individuals* accountable by establishing penalties of both fines and jail time for people who knowingly violate client privacy rights. HIPAA violations are expensive. The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in jail time

What Information is Protected?

HIPAA governs **Protected Health Information (PHI)---**defined as *individually identifiable health information* (IIHI) collected, maintained, used, or disseminated **in any form** by a covered entity. Compliance does not end with the death of the individual, but continues as long as the information is held by the covered entity. This is any information that concerns the past, present or future physical or mental health or conditions of an individual. This includes demographic, clinical, and financial data that either specifically identifies an individual or reasonably could be used to do so.

The HIPAA Privacy Rules specify 18 *personal identifiers* which can individually or in combination be used to identify an individual. For example, a Social Security Number identifies an individual. A name and medical record or health plan member number could be used together to identify an individual. HIPAA protects any such data held by a covered entity. HIPAA does NOT apply to records where the information cannot reasonably be linked to a specific individual, such as when the personal identifiers are coded. (HIPAA *does*, however, apply to the code that links the record data to the personal identifiers.) The 18 personal identifiers under HIPAA are:

1. Complete name, including suffix such Jr., III, etc.
2. Geographic subdivisions (city, state, county, zip codes)
3. Dates directly related to an individual (date of birth, discharge date, date of death, and all specific ages over 89)
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical Record numbers
9. Health Plan Beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URL's)

15. Internet Protocol (IP) addresses
16. Biometric identifiers including finger and voice prints
17. Full face photographic images
18. Any other unique identifying number, characteristic or code

Allowed Use and Disclosure

HIPAA identifies three categories of permissible use of protected health information:

1. use and disclosure for treatment, payment, and health care operations;
2. use and disclosure without authorization for specified purposes;
3. use and disclosure with individual authorization.

Each County department guides employees about appropriate use and disclosure of information within that department's operations.

Use and disclosure for treatment, payment, and health care operations: Unless a client (or employee) specifically objects, covered entities may use protected information and share it with business associates for purposes of providing treatment, arranging for payment, and performing related healthcare operations for the client. For County employees, this may include sharing information with other County departments (whether or not in the covered entity) and with organizations outside county government for treatment, payment, or associated health care operations.

Use and disclosure without authorization for specified purposes: Covered entities may use or disclose PHI without client authorization for certain specific purposes.

- To communicate with a client's family about the client's location, general condition, or death;
- For public health purposes (infection & disease control, child abuse or neglect, reports to Food & Drug Admin);
- Health oversight activity (audits, certifications);
- In response to subpoenas or for judicial & administrative proceedings;

- To law enforcement under certain conditions;
- To coroners and funeral directors;
- For purposes of organ donation;
- For public safety (to prevent threats to health or safety);
- To aid special government functions (military or national security);
- For Worker's Compensation.

For example, County employees may, with client authorization, report diseases, infections or illnesses that are required by law to be reported. Employees may report vital statistics such as births and deaths without client permission. County employees may report suspected or actual child abuse, domestic abuse, neglect or elder abuse to the appropriate authority without client permission. County employees may report pharmaceutical or medical equipment problems to the Food and Drug Administration without client permission.

Use and disclosure with individual client authorization: For all other circumstances, covered entities may use or disclose protected health information only after the client has signed an authorization. Individuals may revoke an authorization (in writing) at any time.

Prohibited Use and Disclosure

County employees are not permitted to:

- give client names or other protected information to a telemarketer without written permission from the client;
- sell the names of clients;
- market medical equipment or supplies to clients;
- market goods and services to our clients.

Notice of Privacy Practices

The County provides a Notice of Privacy Practices to each client at the first face-to-face encounter and obtains the client signature acknowledging receipt. This provides the opportunity to discuss questions on how the County intends to use and/or may disclose PHI. If a client refuses to sign receipt of the Notice, employees must document that a good

faith effort was made to obtain the signature. Talk to your manager about the procedures in your area.

Client Privacy Rights

The HIPAA Privacy Rule establishes standard rights for individuals regarding the privacy and use of their personal health information. These rights must be explained in a Notice of Privacy Practices provided by the covered entity.

- Clients have the right to receive a written copy of Privacy Practices.
- Clients have the right to request restrictions on the use and disclosure of one's own information.
- Clients have the right to receive their health information through confidential means using reasonable alternatives (e.g. mail to a PO Box rather than a street address).
- Clients have the right to inspect and copy their own personal health information. The covered entity may charge a reasonable fee.
- Clients may request an amendment to incorrect or incomplete personal health information. The covered entity is not obliged to comply, but must review the request and communicate an answer to the client within 60 days.
- Clients have the right to request an account of disclosures of their health information by the covered entity. The covered entity does not have to account for disclosures made for treatment, payment, or health care operations; disclosures already authorized by the client; or disclosures allowed without client authorization.
- Clients have the right to file a complaint with the Chester County HIPAA Privacy Officer.

In addition to providing a copy of Privacy Practices, the County must obtain a written and signed consent from the client before using individual health information for any non-covered purpose. The consent must be specific (not a blanket consent), and programs may not deny service to those who refuse to sign.

Personal Representatives

Federal and State laws recognize that some individuals are not capable of making decisions for themselves (e.g. children, mentally incompetent adults, and deceased persons.) Typically, decision-making responsibility for these individuals is legally transferred to someone else, known as a *personal representative* under the HIPAA privacy rules.

1. Children under the age of 18 are usually under the guardianship of one or both of their parents who may act as their personal representative.
2. Mentally incompetent adults may have a court-appointed legal guardian.
3. Deceased persons have executors or next of kin.

The HIPAA Privacy Rule gives personal representatives the same rights and protections as the individual would have for access to and control of personal health information. There are three circumstances when the parent does not have personal representative rights.

1. If state law allows the child to consent to a health procedure, the parent may not be a personal representative for that specific health information.
2. If parental rights have been revoked, the parent is no longer recognized as the child's personal representative.
3. If a parent agrees that the child may have a confidential relationship with a health care professional, the parent is not a personal representative with respect to that provider's records.

Important exception: HIPAA allows covered entities to refuse access and control to a personal representative if the entity reasonably believes such access would endanger the individual (e.g. domestic violence, false medical claims, etc.).

Chester County HIPAA Privacy Officer

Covered entities, including the County, must designate a Privacy Officer to develop, implement, and oversee privacy policies and procedures. These include administrative, technical, and physical safeguards to protect privacy. The Privacy Officer is the central contact for privacy enforcement and complaints.

Thomas Furman

The County of Chester HIPAA Privacy Officer

313 W. Market Street, Suite 6902

West Chester, PA 19380

Phone: 610-344-6190

Fax: 610-344-5998

email: tfurman@chesco.org

Section III – HIPAA Security Rules

HIPAA security rules address external and internal threats to information security including protection from malicious software, hackers, and viruses. The rules outline administrative requirements to assure the safe and secure use and transmission of protected health information, and to protect health information against theft, alteration, or destruction. Included in this is **email encryption** which allows us to exchange PHI for others providing service to our consumers.

Security Safeguards

- **Administrative Rules** – govern employee access to information (paper and electronic), employee training on privacy and security, and procedural security such as passwords, data backup and recovery, and incident reporting.
- **Physical Rules** – security includes facility access, work station security (such as locking workstations and laptop encryption), appropriate use of devices (such as pin numbers on cell phones), internet use, email encryption, etc.

- **Technical Rules**– security includes network firewalls, antivirus processes, data encryption, and audits of hardware and software activity.

A designated Security Officer is responsible for the security of facilities, equipment, electronic personal health information (of employees and clients), and for employee training on security policies.

Chester County HIPAA Security Officer

John Kavak, Chief Information Officer
The County of Chester HIPAA Security Officer
313 W. Market Street, Suite 5302
West Chester, PA 19380
Phone: 610-344-6475
Fax: 610-344-6794
Email: jkavak@chesco.org

Section IV - HIPAA Violation Reporting Requirements

The HIPAA Breach Notification Rule requires notifications to be issued after a breach of unsecured protected health information.

A breach is defined as a use or disclosure of protected health information not permitted by the HIPAA Privacy Rule that compromises the security or privacy of protected health information. Notifications are not required if a HIPAA-covered entity or business associate can demonstrate there is a low probability that PHI has been compromised.

If notifications are required, they must be issued to patients/health plan members 'without unnecessary delay' and **no later than 60 days after the discovery of a breach**.

A media notice must also be issued if the breach impacts more than 500 individuals, again within 60 days. The notice should be provided to a prominent media outlet in the state or jurisdiction where the breach victims are located.

The HHS' Secretary must also be notified within 60 days of the discovery of a breach if the breach impacts more than **500 individuals**, and within 60 days of the end of the calendar year in which the breach was experienced if the breach impacts fewer than 500

individuals. Notify the HIPAA Privacy Officer of any breach **as soon as it is known** so a determination of required notifications can be made.

Section V – Safe Work Practices

Many HIPAA privacy and security practices may be familiar, while others may be new. Here are day-to-day "best practices" for County employees.

Conversation

- Use a quiet voice in the office, on the phone, or whenever discussing client information. Be alert that you may be overheard.
- Avoid speaking about clients in office common areas or building hallways, rest rooms, cafeteria, elevator, etc.
- Never discuss a client in a public setting.

Telephone Use

- If your mobile phone connects to the County network it must be password or pin protected.
- Ask the client for permission to phone them.
- Ask if you may talk to others who may answer the phone.
- Use a quiet voice on the telephone. If possible, select an area where you are less likely to be overheard.

- Do not leave messages with personal health information on answering machines or with anyone but the client.
- When leaving messages, do not identify your department or purpose for calling since this may disclose to others that the person is in services.
- Never discuss a client with the media.
- Discuss telephone protocol with your supervisor for guidance.

Computer Use

- ***Report suspicious email, attachments, or potential viruses to the DCIS Help Desk (x4357, -HELP)***

- Do not share your computer password, not even with a supervisor.
- Arrange your desktop so others cannot easily view the screen.
- Set your computer to "sleep" after a brief idle time.
- Lock or log off your computer when leaving your desk.
- The County email network is secure, so PHI may be emailed with other covered departments but NOT with departments outside the covered entity.
- Do not email PHI to parties outside the County network---the internet is not secure.
- Dispose of all disks or electronic memory devices containing PHI by shredding.

Files

- Do not leave papers/files with PHI in public view.
- Lock files or rooms with PHI when they are not in use.
- Limit access to PHI to employees who must use the information.
- Dispose of papers with PHI by shredding. Do not put in trash or recycling.

Fax

- Avoid using FAX to transmit protected health information when possible. Posted mail often is acceptable, especially for multiple pages.
- Verify the FAX number before transmitting.
- Always use a cover page addressed to a specific individual.
- Never leave sent or received information unattended on the FAX machine.

Social Media

HIPAA was enacted several years before social media networks such as Facebook were launched, so there are no specific HIPAA social media rules. However, there are HIPAA laws and standards that apply to social media use which include any text about specific patients as well as images or videos that could result in a patient being identified. There really is no reason an individual should have to post work related information on a social media account. The County and many departments have a social media presence that is controlled by knowledgeable individuals.

- Best practice is DON'T POST ANYTHING ABOUT A PATIENT\CONSUMER on a personal social media account!