



**TRAINING MANUAL FOR
NEW EMPLOYEES & STUDENTS
OF THE
HEALTH SCIENCES CENTER**

*An Introduction to Privacy & Confidentiality and
Overview of HIPAA Awareness, Policies & Procedures,
Security and Corporate Compliance*

HIPAA IS...

The Health Insurance Portability & Accountability Act of 1996

PORTABILITY

- ✓ Created to ensure access to health coverage
- ✓ Allows for continuity in health coverage
- ✓ Prevents denial due to a pre-existing condition(s)

ACCOUNTABILITY

- ✓ Healthcare fraud is a federal crime
- ✓ Fines and/or jail time may apply
- ✓ Individuals and organizations face sanctions

HIPAA IS HERE...

April 14, 2003 marked the implementation date for compliance with HIPAA's Privacy rule.

FOR YOUR INFORMATION...

Privacy, a component of HIPAA's **Administrative Simplification**, is the first of 3 standards to go into effect.

IN ADDITION...

HIPAA's **Privacy** rule focuses on the safeguarding of patients **Protected Health Information**, ...or **PHI**.

ALSO...

PHI is a culmination of data that is specific to individual patients. This data can be used to identify:

- **a patient**
- **a patient's health**
- **health care services received**

“I.I.H.I.”

Individually Identifiable Health Information are data elements that make up PHI, e.g.;

- Name
- Address
- SSN
- Medical Record Number

SBOHCA

The **S**tony **B**rook **O**rganized **H**ealth **C**are **A**rrangement was set up to facilitate HIPAA compliance. It consists of:

- SBUH
- *schools of the Health Sciences Center*
- members of the Medical Staff
- employees and contracted professionals of the PC’s
- faculty practices

- ✓ SBOHCA collects health information and stores it in electronic and written formats.
- ✓ Health information is the property of SBOHCA but is accessible by the patient.
- ✓ SBOHCA can use the information for TPO purposes.

TPO

Treatment – Health information can be used or disclosed to provide medical treatment.

Payment – Health information can be used or disclosed to enable entities to receive payment for medical services provided

Operations – Health information can be used or disclosed for operational purposes (clinical education, utilization review, etc.)

WRONGFUL DISCLOSURE:

- **EXAMPLE #1:**

In North Carolina, a company fired a good worker after it had learned that the employee tested positive for a genetic illness that could have led to lost work time and increased insurance costs.

- **EXAMPLE # 2:**

In California a woman sued a pharmacy that released her medical information to her husband who used it to damage her reputation in a divorce proceeding.

- **EXAMPLE # 3:**

After visiting her mother at work, the teenage daughter of a hospital employee took a list of patient names and phone numbers and for fun, called the patients to tell them that they were diagnosed with HIV.

THE CHANGING FLOW OF INFORMATION

- ✓ In the past, health information contained in paper records would have been difficult to remove and make use of outside of an organization.
- ✓ Today, electronic storage of data and email allows for information to travel at record speeds.
- ✓ With advances in technology come the potential for misuse and abuse.

OUR COMMITMENT TO PRIVACY

- ✓ Every institution has a commitment to protect patient privacy.
- ✓ 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.
- ✓ The *Office of Civil Rights* within the *DHHS* has the authority to enforce these rules.

PRIVACY GOALS

- ✓ We need to maintain trust with our patients.
- ✓ Patients will be educated as to their rights.
- ✓ The safeguarding of patient's **PHI** is at the cornerstone of HIPAA's privacy rule.

WHAT ARE THE LIMITS?

PHI will be limited to those who need the information to:

- ✓ provide care (**T**reatment)
- ✓ handle payment (**P**ayment)
- ✓ manage health care operations (**O**perations)

AUTHORIZATION

- ✓ Authorization is required when disclosing PHI for purposes other than treatment, payment or operations.

EXAMPLE:

Breast Care Center wants to use the names of "survivors" for their latest marketing campaign.

(Patients have the right to revoke their authorization.)

The Exception...

A hospital may disclose PHI without patient authorization to further certain public policy objectives including:

- For judicial or administrative proceedings;
- For health oversight activities;
- For law enforcement purposes;

WHAT IS PROTECTED?

HIPAA protects communications that are:

- ✓ spoken
- ✓ written
- ✓ electronic

SPECIAL NOTE...

A hospital may not be restricted on the use of:

de-identified information

NEED TO KNOW

- ✓ Privacy is not a new concept in health care.
- ✓ Under HIPAA's **new** privacy rule it will be a ***federal crime*** to violate this principle.
- ✓ Privacy rules are not limited to the healthcare industry.

TO WHOM DO HIPAA RULES APPLY?

Covered Entities are bound by the guidelines.

These would include;

- Health care providers
- Health care clearinghouses
- Health plans

HOW IS HIPAA ENFORCED?

- ✓ Civil penalty for **inadvertent** violation = fines of \$100/per incident up to \$25,000/per year for each similar offense.

Example #1:

A hospital violates HIPAA by disclosing 100 patient records. The hospital has to pay a \$10,000 fine.

- ✓ Criminal penalties = large fines + jail time, and **increase** with the degree of the offense.

SPECIAL NOTE:

Selling patient information for personal profit is not the same as accidentally allowing the information to be released. Criminal penalties could be as much as **\$250,000 and/or 10 years in jail.**

OUR FOCUS

- ✓ SBOHCA has enacted a series of **P&P** that will provide guidance on a number of critical areas covered under the rule.
- ✓ This manual will help to familiarize staff and students with several key items that are of major concern.

PATIENT'S RIGHTS AND RESPONSIBILITIES

- ✓ Patient has the right to:
 - request restricted use and disclosure of PHI;
 - inspect and copy their health information.
 - request to amend their medical record.

PATIENT RIGHTS...

- ✓ SBOHCA has the responsibility to inform patients as to their rights and the manner in which to exercise these rights.
- ✓ Inpatients shall be given information at admission.
- ✓ Outpatients will be given information at their first registration.
- ✓ Reasonable accommodations shall be made to persons with communication impairments and LEP.
- ✓ ***Patient & Guest Relations Department*** has the charge to oversee patient rights.

PATIENT REQUEST TO AMEND PHI

- ✓ HIPAA gives a patient the right to request a change to their **PHI** contained in health records.
- ✓ Patients should be directed to submit all requests to the ***HIM Department***.
- ✓ All requests must be made in writing with supporting backup documentation.
- ✓ SBOHCA will review the request(s) and, within 60 days, make a decision as to whether to honor or deny said request.

FACILITY DIRECTORY/CENSUS

- ✓ At registration, patients will be given an opportunity to be included in the hospital's database.
- ✓ If the patient "**opts in**", he/she has the right to decide what type of information can be given out (i.e. room #, religious affiliations, etc.)
- ✓ If a patient "**opts out**" the objection must be recorded and the appropriate "status" must be noted in the directory.
- ✓ The *Admitting Department* will forward census information to the patient's unit for inclusion in the medical record.

MINIMUM NECESSARY FOR USE AND DISCLOSURE OF PHI

- ✓ Employees and students must limit their access of **PHI** to the minimum amount that is needed to perform a job function.
- ✓ Computer sign-on and overall access to **PHI** will be determined by the scope and responsibilities of an employee's and student's role.

Notify your department manager if you believe that in the course of your duties, you are approached with a non-routine situation.

INCIDENTAL DISCLOSURES

Incidental disclosures are not considered a violation of the regulations as long as the minimum necessary standard is met and reasonable safeguards are in place.

- ✓ **EXAMPLE:**
Sign-in sheets, and overheard conversations.

FAXING of PHI

- ✓ SBOHCA staff must take reasonable measures to protect **PHI** that is faxed.
- ✓ Fax only the minimum necessary amount of information and ensure that it reaches the intended recipient.
- ✓ Whenever possible, avoid faxing sensitive information.

EMAIL USAGE

Can **PHI** be transmitted via email?

**EMPLOYEES AND STUDENTS ARE NOT ALLOWED TO SEND PHI
OUTSIDE OF LOTUS NOTES!!!**

HANDLING AND DISPOSAL OF DISCARDED MATERIALS

- ✓ Secure, lockable containers will be used to collect all discarded materials.
- ✓ These containers will be used to deposit office papers, folders, computer disks.
- ✓ Private contractor (**only**) will be responsible for removing the contents of these containers.

ACCOUNTING OF DISCLOSURES

- ✓ Patients have a right to a full accounting and disclosure when their **PHI** is used for purposes above and beyond **TPO**.
- ✓ **SBOHCA** has to track all such disclosures and be prepared to honor a patient's request.
- ✓ Examples of the types of disclosures to be tracked include disclosures made to health services such as;
 - **birth certificates**
 - **death certificates**
 - **infectious disease reporting**
- ✓ Accounting of disclosure **is not** needed when the disclosure was made;
 - **to the patient**
 - **when authorized by patient**
 - **for TPO**
 - **prior to April 14, 2003**

HIPAA SECURITY

WHAT IS SECURITY?

Steps taken to protect against potential threats.

HIPAA SECURITY...

Focus on 3 types of safeguards:

- ✓ Administrative
- ✓ Physical
- ✓ Technical

ADMINISTRATIVE SAFEGUARDS

What policies and procedures do we have in place to protect E-PHI?

TECHNICAL SAFEGUARDS

How can we use technology to protect E-PHI?
(i.e., computer software that tracks and flags unauthorized users)

PHYSICAL SAFEGUARDS

How will we protect our physical infrastructure?
(i.e.; buildings and equipment)

CONSEQUENCES FOR SECURITY BREACH:

- Patient safety/medical care is compromised
- Negative publicity
- Increased costs
- Identity theft
 - Patients can become targets of con artists
- **Legal liability/lawsuits**

COMBAT THE THREAT

- ✓ Log off of the computer system before you walk away.
- ✓ Re-position computer monitors so that passerbys cannot view the information.
- ✓ Do not share passwords.

SECURITY SCENARIO

It has been the practice to leave the records system open and logged on at the nurses station computer at the end of a shift. This saves time during shift changes for staff who need to retrieve records.

Is this an appropriate practice under HIPAA?

It may seem like a timesaver but this practice is equivalent to sharing a password. When others are allowed to access the system under your password, there can be no way to audit who sees the records and when.

SPECIAL NOTE...

CHOOSE A “STRONG” PASSWORD

Examples

- ✓ WEAK PASSWORD: MARY67
- ✓ STRONG PASSWORD: 2Bon2Bti?

BALANCING ACT

- ✓ There is an inverse relationship between **convenience** (ease-of-use) and **security**.
- ✓ As you increase security, you lose **convenience**.

WORKFORCE CONFIDENTIALITY AGREEMENT

- ✓ Many healthcare employees and students have access to highly personal and sensitive patient information.
- ✓ Federal and state law requires that SBOHCA protect and preserve the confidentiality of a patient’s information.
- ✓ By signing the WCA, employees and students are committing to the adherence of specific requirements related to patient confidentiality.

“WHAT DO I NEED TO DO?”

- ✓ Review HIPAA/Compliance related policies
- ✓ Do not be afraid to ask questions about departmental practices
- ✓ Identify risk areas within your department

REPORT SECURITY VIOLATIONS

- ✓ Security Officer
- ✓ Compliance Officer
- ✓ University Counsel
- ✓ **Compliance Hotline (631) 444-6666**

SBOHCA HIPAA Website

<http://inside.hospital.stonybrook.edu/sbuh/sbuhhipaa>

CORPORATE COMPLIANCE TRAINING 2004

Compliance is Everyone's Responsibility

THE NEED FOR COMPLIANCE IN HEALTHCARE

- ✓ Healthcare Billing Fraud results in the loss of millions of tax \$'s each year to Medicare and Medicaid scams.
- ✓ Growing concern that the Medicare System will go bankrupt particularly with the Baby Boomers entering retirement within the next 10 years.
- ✓ Major public demand for reform without tax increases
- ✓ Increasing regulatory complexity and governmental oversights.

FRAUD IN HEALTHCARE: BRIEF HISTORY

- ✓ Hospitals and Healthcare Providers were once paid according to their "reasonable cost".
- ✓ Waste, fraud and abuse became rampant in the industry.
- ✓ Laws and regulations were developed to combat this abuse.
- ✓ Government mandated financial consequences would push providers towards delivering care in a more cost efficient/effective manner.

FRAUD DEFINED

- ✓ Unintentional errors (mistakes)
- ✓ Fraud and abuse

WHY CREATE A COMPLIANCE PROGRAM?

- ✓ Foster a culture that promotes legal and ethical behavior
- ✓ Enable the hospital to manage areas of potential regulatory compliance risks
- ✓ Improve overall quality of care and operational efficiency

WHAT DOES IT DO?

- ✓ Defines the conduct expected of Hospital Representatives
- ✓ Provides guidance on how to resolve questions regarding legal and ethical issues
- ✓ Establishes a reporting mechanism for possible violations

WHAT ARE ITS KEY FEATURES?

- ✓ The “Code of Conduct” and the “Ethics in Compliance Guide”
- ✓ A Corporate Compliance Officer and Compliance Committee to carry out the program
- ✓ Periodic education training sessions to discuss specific areas of compliance
- ✓ Annual auditing, reviews and monitoring activities

ASK YOURSELF...

- ✓ Is my action consistent with hospital practices and policies?
- ✓ Does my action appear improper?
- ✓ Does it meet my personal code of behavior?
- ✓ Can I defend my action to a supervisor, other employees and to the general public?

COMPLIANCE PROGRAM DESIGN

- ✓ Our program is modeled after program guidance from the Department of Health and Human Services Office of the Inspector General (HHS OIG).
- ✓ The Program has 7 basic elements.
- ✓ **A Key Element** = Delegation of Authority: Not to individuals bent towards illegal activities.

CIVIL LAW EXAMPLES

- ✓ **False Claims Act (FCA)**
- ✓ **Civil Monetary Penalty Law (CMPL)**
- ✓ False Statement Statute
- ✓ Whistleblower Suits

CIVIL LAW VIOLATION CONSEQUENCES

- ✓ Repayment of Overpayment (max. 3 X's amount)
- ✓ Penalty of \$5,000 - \$10,000 per false claim
- ✓ Exclusion from Medicare and Medicaid program

ACADEMIC MEDICAL CENTER
FRAUD SETTLEMENTS

- ✓ **Stony Brook University Hospital - \$850,000**
- ✓ **Howard University - \$1.8 million**
- ✓ **Mt Sinai School of Medicine - \$2.3 million**
- ✓ **Georgetown University - \$5.0 million**
- ✓ **Yale University - \$5.6 million**
- ✓ **University of Virginia - \$8.4 million**
- ✓ **Montefiore Medical Center - \$12 million**
- ✓ **Thomas Jefferson University - \$12.5 million**
- ✓ **University of Pittsburgh - \$17 million**
- ✓ **University of Texas at San Antonio - \$17.2 million**
- ✓ **Staten Island University - \$80 million**

CRIMINAL LAW EXAMPLES

- ✓ **Health Care Fraud - submission of false claims**
- ✓ **Wire Fraud - electronic submission of false claims**
- ✓ **Mail Fraud – mailing of false claims**

CRIMINAL LAW VIOLATION CONSEQUENCES

- ✓ **Suspension/revocation of professional license**
- ✓ **Automatic exclusion from Government Health Programs**
- ✓ **Imprisonment**

HOW DOES THE GOVERNMENT DECIDE WHO IS CULPABLE?

“KNOWS OR SHOULD KNOW”

- ✓ **Acts with knowledge.**
- ✓ **Acts in deliberate ignorance of the truth.**
- ✓ **Acts in reckless disregard of the truth.**
- ✓ **Specific intent to defraud is not required.**

STANDARDS OF CONDUCT

- ✓ Ethical Business Practices
- ✓ Safeguard Our Assets & Environment
- ✓ Quality Care
- ✓ Human Resources

ETHICAL BUSINESS PRACTICE

- ✓ Refrain from Misrepresentations (keep it honest)
- ✓ Submit Accurate Billings & Financial Reports
- ✓ Ensure Proper Use of Hospital Assets
- ✓ Prevent Unlawful Referrals and Kickbacks
- ✓ Avoid Conflicts of Interest
- ✓ Ensure Appropriate Use of Hospital Information

SAFEGUARDING OUR ASSETS & ENVIRONMENT

- ✓ Comply with Environmental Health and Safety Requirements
- ✓ Prevent inappropriate Gifts and Entertainment

ETHICS SCENARIO...

Ann Smith is a Nursing Assistant who really enjoys her job. She consistently performs duties well, and with great pride. The patients and their families truly appreciate Ann's good efforts. Mr. Jones is being discharged today and as a token of his gratitude offers Ann a diamond pendant.

Should she accept this gift?

- ✓ Ann should tactfully refuse the gift.
- ✓ State ethics law restricts gifts that value \$75 or more
- ✓ Avoid the appearance of impropriety... (i.e., favors can be bought)

QUALITY CARE

- ✓ Provide Emergency Care
- ✓ Ensure Proper Control of Medications

DRUG DIVERSION POLICY

- ✓ DOH requires monitoring and reporting of drug diversion within hospitals.
- ✓ Drug Diversion is a violation of state and federal laws regarding controlled substances.
- ✓ Consequences go beyond loss of employment: Criminal charges may apply.
- ✓ At-risk individual can find resources available through the Employee Assistance Program (EAP).
- ✓ All concerns will be handled in a confidential manner.

HUMAN RESOURCES COMMITMENT TO FAIRNESS

- ✓ Equal opportunity employment
- ✓ Reasonable accommodations for persons with disabilities
- ✓ Zero tolerance for Sexual Harassment

SEXUAL HARASSMENT POLICY

- ✓ Definition: Unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature.
- ✓ Such conduct creates an intimidating, hostile or offensive working environment.
- ✓ Stony Brook Hospital & the HSC adhere to a campus-wide sexual harassment policy.
- ✓ *Human Resources and the Office of Diversity and Affirmative Action* resolve all issues.

WHO SHOULD COMPLY?

- ✓ Hospital employees
- ✓ Medical staff
- ✓ Faculty members
- ✓ Independent Contractors
- ✓ Vendors
- ✓ All others representing the Hospital (i.e., HSC staff, PC employees, students)

REPORTING OF POSSIBLE VIOLATIONS

- ✓ **Where to Report** – Immediate Supervisor, Departmental Chain of Command, or Compliance Office.
- ✓ **What to Report** – An actual or reasonable belief of a violation.
- ✓ **Consequences of Reporting** – No retaliation or discipline for reporting in good faith.
- ✓ **Investigations of Violations** – All allegations of wrongdoing will be assessed and investigated.
- ✓ **Discipline for Violations** – In accordance with existing collective bargaining agreements.

COMPLIANCE HOTLINE

- ✓ Call when you feel your concerns cannot be communicated through normal processes.
- ✓ Calls can be made anonymously.
- ✓ Calls cannot and will not be traced.
- ✓ Calls will be investigated.
- ✓ **Calls can be made to (631) 444-6666.**

AS A WRAP UP...

- ✓ Comply with all legal and regulatory requirements
- ✓ Keep accurate records
- ✓ Behave ethically
- ✓ Comply with the Conflict of Interest Policy
- ✓ Report possible violations

UNIVERSITY HOSPITAL'S CORPORATE COMPLIANCE OFFICE

- ✓ The Corporate Compliance Officer is Robert G. Eaton
- ✓ Compliance Officer reports to the Director/CEO and the Governing Body of the Hospital.
- ✓ The Compliance Office is located at 3 Technology Drive, Suite 200.
- ✓ **The phone number is (631) 444-5776.**

☺ **Thank you for completing this training program. Please detach, complete and sign both the Acknowledgement Form and the Workforce Confidentiality Agreement.**