



HIPAA In The Workplace

What Every Employee Should
Know and Remember

[What is HIPAA?]

The Health Insurance Portability and Accountability Act of 1996

Portable

Accountable

Rules for Privacy

Rules for Security

<http://www.hhs.gov/ocr/privacy>

Health Information Privacy

- Office for Civil Rights
- Civil Rights
- Health Information Privacy**

[OCR Home](#) > Health Information Privacy

- HIPAA**
 - [Understanding HIPAA Privacy](#)
 - [HIPAA Administrative Simplification Statute and Rules](#)
 - [Enforcement Activities & Results](#)
 - [How to File a Complaint](#)
 - [Frequently Asked Questions](#)
 - [News Archive](#)
- PSQIA**
 - [Understanding PSQIA Confidentiality](#)
 - [PSQIA Statute & Rule](#)
 - [Enforcement Activities & Results](#)
 - [How to File a Complaint](#)

Health Information Privacy

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information, and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule

[Learn about](#) the Privacy Rule's protection of the privacy of individually identifiable health information, the rights granted to individuals, OCR's enforcement activities, and how to file a complaint with OCR.



OCR Privacy Listserv

Learn more about the Privacy Rule! Sign up for the [OCR Privacy Listserv](#).

What's New in Privacy

- > [GINA Notice of Proposed Rulemaking](#) - 10/1/09
- > [New Breach Notification Web Pages](#) - 9/23/09
- > [Patient Safety Rule Penalty Inflation Adjustment](#) - 8/25/09
- > [HITECH Breach Notification Interim Final Rule](#) - 8/19/09
- > [Regional Office Privacy Advisors](#) - 8/14/09
- > [Secretary Delegates HIPAA Security Rule to OCR, Press Release](#) - 8/3/09

The Patient Safety and Quality Improvement Act of 2005 (PSQIA) Patient Safety Rule

[Learn about](#) the Patient Safety Rule's protection of confidential patient safety work product, the permitted disclosures of patient safety work product, OCR's enforcement activities, and how to file a complaint with OCR.



[Privacy Effective Dates:]

April 14, 2003

Privacy Rules effective this date

Compliance Date

Regulations enforced by the Office of
Civil Rights

[What is the Privacy Regulation?]

Intention of the regulation is to protect health information from non-medical uses by employer, marketers, etc.

Regulate access to individuals health information

Information that is not in electronic format is protected under privacy

What is Protected Health Information (PHI)?

Any Information, in any medium that:
Relates to the past, present or future
physical or mental health or condition or
provision of, or payment for health care to
an individual AND
created or received by health care
provider, health plan, public health
authority, employer, life insurer, state
agency.

What makes it personally identifiable?

Health Information including demographic data collected from an individual that:

Permits identification of the individual or

Could reasonably be used to identify that individual

Examples: Name, Address, ID Number, Job Classification, Zip Code, Age, Job Tenure, Photo, Education Level, etc.

If it is personally identifiable- IT IS PROTECTED!!

[What PHI Will You See?]

Member Records

FMLA Requests

Enrollment Forms

Authorizations

AASIS

Who must comply with the HIPAA Regulations?

Hospitals, insurance companies, physician offices, private companies and state agencies

Employee Benefits Division of the Department of Finance and Administration and their Business Affiliates/Associates

[Am I a Business Associate?]

Yes, if you do business with EBD you are a Business Associate.

Business Associates are now subject to all provisions of HIPAA Privacy and Security.

Business Associates are now subject to the same Civil and Criminal Penalties as Covered Entities

Protected Health Information (PHI) Permitted Uses and Disclosures:

You must have a signed authorization in order to disclose PHI

You must identify employees who may receive PHI

You must only divulge minimum necessary information

You must have an effective mechanism to resolve employee non-compliance

Who is responsible for authorization, and when do we need it?

Authorization is required for any use or disclosure that is not related to treatment, payment or healthcare operations related activities

Entity that has the information must have authorization **PRIOR** to disclosure

[HIPAA Security Effective Dates:]

Effective April 14, 2005

Security Rules effective this date

Compliance Date

Regulations enforced by the Office of
Civil Rights as of August 3, 2009

What is the Security Regulation?

Ensure the confidentiality, integrity and availability of all electronic protected health information

Protect against any reasonably anticipated threats and uses or disclosures that are not allowed by Privacy regulations

Electronic format such as emails covered under security

What is the Security Regulation?

No permitted “incidental” disclosures or uses under Security

Evaluation, review and updating of documentation is required

Mitigate these threats by whatever safeguards you believe can be “reasonably and appropriately” be implemented in line with Security regulation

[What makes it electronic PHI?]

Electronic PHI- PHI transmitted or maintained on electronic media:

Electronic storage media, including memory devices in computers, thumb drives, etc.

Transmission media used to exchange information already in electronic storage media, such as email

Certain transmissions, including of paper via fax, and voice are not considered transmissions via electronic media

[What does HIPAA allow us to do?]

Treatment
Payment
Operations
(TPO)

[Unsecure PHI]

PHI in any medium (electronic, paper or oral) that is not secured through use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Only form of “secure” PHI is encryption or shredding (cross-shredding)

[What is a Breach?]

Anything that compromises the security or privacy of protected health information (PHI) and

Poses a significant risk of financial, reputational, or other harm to the individual

Unauthorized acquisition, access, use, or disclosure of PHI is considered a breach of PHI

What do I do If I think a Breach has Occurred?

Contact EBD as soon as you receive notification

No later than 24 hours of discovery of breach

Must provide identity of each individual whose unsecured PHI has been or is reasonably believed to have been breached

Genetic Information Non-Discrimination Act (GINA)

Title I part of Privacy Rule as of
October 2009

Can not use Genetic Information to
discriminate for basis of health
insurance enrollment or underwriting

Can not use Genetic Information to
discriminate in employment decisions
(Title II)

[Most Frequent Complaints:]

Lack of adequate safeguards

Disclosures not limited to “minimum necessary” standard

Failure to obtain authorization

What Happens with Non-Compliance?

Entity did not know (even with reasonable diligence): Minimum penalty \$100 per violation (\$25,000 per year for violating same requirement) up to \$50,000 per violation (up to \$1,500,000 annually)

Reasonable cause, not willful neglect: Minimum penalty \$1,000 (\$100,000) up to \$50,000 (\$1,500,000 annually)

What Happens with Non-Compliance?

Willful neglect, but corrected within 30 days:
Minimum penalty \$10,000 per violation
(\$250,000 per year for violating same
requirement) up to \$50,000 per violation (up
to \$1,500,000 annually)

Willful neglect, not corrected: Minimum
penalty \$50,000 (\$1,500,000) no maximum
annual penalty

Jail time can be associated depending on
the nature of the offense

Attorney General Prosecution

The State Attorney General has the authority as of 2/2009 to bring action on the behalf of residents in their state to stop violations and/or obtain damages of \$100 per violation not to exceed \$25,000 per year for similar violations. State can recover attorney fees in any civil action to collect damages

[As a Supervisor- What can you do?]

You can ask (Why are you not coming to work today?)

You can request additional information

You must protect that information

Information can be shared vertically (with your boss, but not your co-workers)

[4 ways to secure your workstation]

Lock up

Always Log out of your Systems

Disable your drives (done by Tech Support)

Make Security a part of your Routine

[3 ways to eliminate unauthorized use]

Use workstation ID's and passwords

Use screen savers

Position your monitor away from doorways and windows

If you have any doubt whether HIPAA applies:

Don't say anything, or say the
minimum necessary

Contact the Compliance Department

Procedural Safeguards:

Visits to secured areas should be limited to business purposes only

NEVER recycle anything containing
PHI- ALWAYS shred PHI

Be careful with faxed claims data – it is the most at risk for breach of privacy

Security Examples

If I do not object, can my health care provider share or discuss my health information with my family, friends, or others involved in my care or payment for my care?

Security Examples

Can my Doctor or Nurse discuss my health information or condition with my brother if I tell them not to?

Security Examples

Wal-Mart

Anne Presley's Medical Record (6 Employees dismissed from St. Vincent's)

NW AR Nurse received 2 years probation and 100 hours community service

Questions?



© 2003 United Feature Syndicate, Inc.