

# IMPLEMENTING HIPAA PRIVACY



# Privacy

---

## Traditional

- Paper Records
- State-governed
- Providers, plans
- Release

## HIPAA

- Info. in any form
  - Federal regulation
  - Business associates
  - Use and disclosure
-

# State Law Preemption

---

**HIPAA = Federal floor of privacy protection**

**May have more stringent state laws or facility policies.**



# Privacy – Key Changes

---

- **Consent optional**
  - **Expanded disclosures for treatment, payment, health care operations**
  - **Incidental disclosures not a violation**
  - **Simplify authorizations**
  - **Additional time for BA contracts**
  - **Simplify marketing provisions**
  - **Further limit accountings**
-

# Covered Information

“Protected health information” (PHI)

- Individually identifiable health information that is maintained in any form or medium.



# Key Privacy Issues

---

- **Permission necessary for use or disclosure**
- **Minimum necessary**
- **Business associates**
- **Patient rights**
- **Administrative requirements**



# HIPAA is Reasonable!

---

- “. . . the Privacy Rule must not impede essential health care communications and practices.”
  - Incidental disclosures are not violations
-



# Permission Necessary for Use or Disclosure of PHI



# Use and Disclosure of PHI

---

## General Rule

A health care provider may not use or disclose PHI, except as required or permitted by the regulations.

---

# Required Disclosures

---

- **To the subject of the information**
  - **To HHS**
-

# Permissible Uses & Disclosures: Permission Necessary

---

- **Optional Consent**
  - **Opportunity to agree or object**
  - **No permission required - Public policy**
  - **Authorization**
-



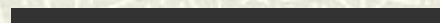
---

***Distinguish:***

**Consent to treat**

**vs.**

**Consent to use or disclose PHI**



# Optional Consent

---

**No patient permission is required to use or disclose PHI for Covered Entity's:**

- **Treatment**
- **Payment**
- **Health care operations**

*But CE may obtain Consent if desired*

---

# Treatment

---

**Provision, coordination, management of health care and related services, including:**

- **Coordination with a third party**
  - **Consultation between providers**
  - **Referral**
-

# Payment

---

**Activities to obtain reimbursement for the provision of health care, including:**

- **Eligibility determination**
  - **Billing**
  - **Claims management**
  - **Medical necessity review**
  - **Utilization review**
-

# Health Care Operations

---

## Examples:

- **Quality improvement**
  - **Evaluating performance**
  - **Training programs**
  - **Business management activities**
-

# Disclosures to Other Entities

---

**No permission is required to disclose PHI for:**

➤ **Treatment by another provider**

➤ **Payment of:**

**Another Covered Entity**

**Another provider**

➤ **Health Care Operations of another CE if:**

**Relationship with patient**

**Purposes of QI or fraud and abuse detection**

---

# Notice of Privacy Practices

---

Consent optional, but must make a *good faith effort* to obtain patient's *written acknowledgement* of receipt of Notice of Privacy Practices.



# Notice of Privacy Practices

---

**Required elements include:**

- **Mandated header**
  - **Permitted and required uses and disclosures of PHI**
  - **Individual rights**
  - **Provider's duties**
  - **Complaint process**
  - **Contact person**
-

# Opportunity to Agree or Object

---

**Verbal permission to use or disclose PHI is sufficient if the individual is:**

- **Informed in advance**
  - **Given the opportunity to agree, prohibit or restrict disclosure**
-

# Opportunity to Agree or Object – When Allowable

---

- Facility directories (inpatient)
- Persons involved in care or payment
- Notification of family
- Disaster relief

*If opportunity to object cannot be given –  
best interests of individual*

---

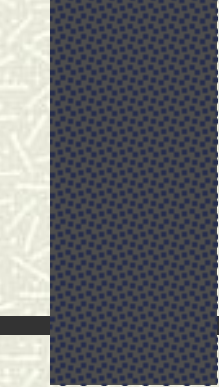
# No Permission Required – Public Policy

---

- **Required by law**
- **Work Comp**
- **Public health activities**
- **Abuse, neglect reports**
- **Health oversight activities**
- **Judicial and admin. proceedings**

**(cont.)**

---

- 
- 
- **Law enforcement**
  - **Coroners, medical examiners & funeral directors**
  - **Organ donation**
  - **Research, with IRB approval**
  - **Necessary to avert serious threat**
  - **Specialized government functions**
-

# Authorization

---

**Prior, written, specific Authorization of the individual is required to use PHI for:**

- **Psychotherapy notes**
  - **All uses and disclosures not otherwise permitted or required**
-

# Authorization Examples

---

- **Attorneys**
  - **Relatives** (*involved in treatment or payment?*)
  - **Life insurance**
  - **Schools, camps**
  - **Employers**
  - **Marketing**
  - **General fundraising**
-



# Minimum Necessary

Just the  
facts,  
Ma'am...



# Minimum Necessary

---

Providers must make reasonable efforts to limit requests for, and disclosures of, PHI to the **minimum necessary** to accomplish the intended purpose.

---

# Minimum Necessary - Exceptions

---

**Does not apply to disclosures:**

- **To health care providers for treatment**
  - **To the subject of information**
  - **To HHS**
  - **Required by law**
  - **Authorized by patient**
-

# Minimum Necessary - Requirements

---

- Limit staff access to PHI
- Implement policies for routine uses disclosures
- For non-routine disclosures:
  - Develop criteria
  - Review requests on an individual basis

*Flexibility in implementation*

---



# **Business Associates**



# Business Associates

---

- Provide services on your behalf involving disclosure of PHI, or
- Perform functions involving disclosure of PHI

e.g.:

- Legal
- Billing
- Consulting
- Accreditation
- Accounting
- Claim processing
- Management
- Financial services
- UR
- Data aggregation

# Business Associates

---

- Provider must obtain “satisfactory assurance” that business associates will appropriately safeguard PHI
- Satisfactory assurance = contract
- HHS Model Business Associate Contract

*Additional time to implement some BA contracts*

---

# Business Associates

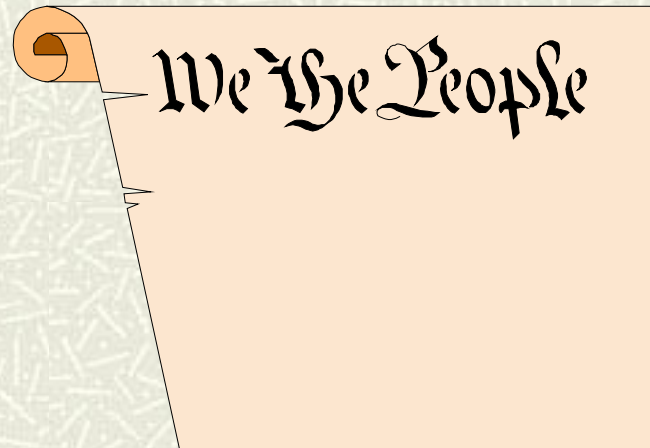
---

**Business associates do not include:**

- Members of workforce**
  - “Conduits” (e.g., USPS, Federal Express)**
  - Physician/hospital (staff privileges)**
  - Provider/payer**
-



# Patient Rights



# Patient Rights

---

- **Notice of Privacy Practices**
  - **Request restrictions on uses and disclosures**
  - **Access to inspect and copy**
  - **Amendment**
  - **Accounting of disclosures**
-



# Administrative Requirements



# Admin. Requirements

---

- Documented policies and procedures
  - Privacy official
  - Privacy training
  - Complaint process
  - Sanctions for violations
  - Mitigation of harm
  - Refrain from retaliatory acts
  - Administrative, technical & physical safeguards
-

# Privacy Deadline

---

April 14, 2003



