

HIPAA Basics for Physicians

**The 123rd Annual Meeting of the
LSMS House of Delegates**



Administrative Simplification Overview

Administrative Simplification Overview



Administrative Simplification Overview

History

- Clinton Proposal
 - Uninsured
 - Cost
 - Middle class concerns
- Incremental reform
 - Health Insurance Reform Act of 1995 (a/k/a the Kennedy-Kassebaum Health Care Reform Bill)



Administrative Simplification Overview

PUBLIC LAW 104-191

AUG. 21, 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.



Administrative Simplification Overview

HIPAA included:

- Administrative Simplification
 - intended to reduce cost
- Privacy regulation
 - intended to protect rights



Administrative Simplification Overview

Subtitle F—Administrative Simplification

SEC. 261. PURPOSE.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.



Administrative Simplification Overview

General Requirements

- **Applicability**
 - “Covered Entities”
 - health plans
 - health care clearing houses
 - healthcare providers who transmit electronically
- **Reduction in cost**



Administrative Simplification Overview

Covered Transactions

- (A) Health claims or equivalent encounter information.
- (B) Health claims attachments.
- (C) Enrollment and disenrollment in a health plan.
- (D) Eligibility for a health plan.

(Continued)



Administrative Simplification Overview

Covered Transactions *(continued)*

- (E) Health care payment and remittance advice.
- (F) Health plan premium payments.
- (G) First report of injury.
- (H) Health claim status.
- (I) Referral certification and authorization.



Administrative Simplification Overview

Standards To Be Set

- Unique Health Identifiers
- Transaction & Code Sets
 - “... from among the code sets that have been developed by private and public entities”
- Security Standards
- Electronic Signatures
- Transfers ... Among Health Plans



Administrative Simplification Overview

Compliance Time Frames

- **Employer Identifiers**
 - Final rule published May 31, 2002
 - Effective date July 30, 2004
- **Provider Identifier**
 - Proposed rule published July 6, 1998
- **Health Plan and Individual Identifiers**
 - Not yet finally published



Administrative Simplification Overview

Compliance Time Frames

- **Transaction & Code Set Rule**
 - Final rule published August 17, 2000
 - Extension deadline October 15, 2002
 - Effective date October 16, 2003
- **Security**
 - Proposed in August 12, 1998
 - Not yet finally published
- **Privacy**
 - Final Rule published December 28, 2000
 - Effective April 14, 2003



Administrative Simplification Overview

Penalties

- “Violations” - \$100 each, up to \$25,000 per year
- “Wrongful” use or disclosure - \$50,000 and/or up to 1 year
- “Under false pretenses” - \$100,000 and/or up to 5 years
- “Commercial” or “malicious” - \$250,000 and/or up to 10 years



Administrative Simplification Overview

Privacy

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(c) REGULATIONS.—

(1) IN GENERAL.--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).



Administrative Simplification Overview

Privacy

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(c) REGULATIONS.—

(2) PREEMPTION.--A regulation promulgated under paragraph (1) shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.



HIPAA Privacy

Privacy Regulations



HIPAA Privacy

Five Basic Features of Privacy Regulations

1. No use or disclosure unless permitted
2. Permitted uses & disclosures
3. Other patient rights
4. Administrative requirements
5. Technical provisions



HIPAA Privacy

Five Basic Features of Privacy Regulations

1. No use or disclosure unless permitted
 - A. The "Basic Rule"
 - B. Specific Disclosure Issues



HIPAA Privacy

Five Basic Features of Privacy Regulations

2. Permitted Uses/Disclosures

- A. For treatment, payment and healthcare operations (formerly “consent”) (§506)**
- B. With authorization (§508)**
- C. “Opt-opt” situations (§510)**
- D. Exceptions (§512)**
- E. Patient (§524)**



HIPAA Privacy

Five Basic Features of Privacy Regulations

3. Other Patient Rights

- A. Notice of privacy protections (§520)**
- B. Requests for additional protections (§522)**
- C. Access (inspection and copying) (§524)**
- D. Amendment (§526)**
- E. Accounting for disclosures (§528)**



HIPAA Privacy

Five Basic Features of Privacy Regulations

4. Administrative Requirements (§530)

- A. privacy officer
- B. training
- C. safeguards & security
- D. complaints to the covered entity
- E. policies and procedures
- F. documentation
- G. sanctions
- H. verification



HIPAA Privacy

Five Basic Features of Privacy Regulations

5. Miscellaneous Provisions

- A. Preemption of State Law (160 CFR 201 et seq.)
- B. Compliance and Enforcement (160 CFR 300 et seq.)
- C. Transition provisions (§532)



HIPAA Privacy

Privacy Regulations – Selected Issues



HIPAA Privacy

1. No use/disclosure unless permitted

- “A covered entity may not use or disclose an individual’s protected health information, except as otherwise permitted or required by this subpart.”

§ 164.502(a).

- What is “protected health information”?



HIPAA Privacy

1. No use/disclosure unless permitted

– Specific Disclosure Issues

a. Organizational Issues (§504)

- Hybrids and healthcare components
- Affiliates
- Business associate contracts

b. Disclosure Issues

- De-identification (§514)
- Minimum necessary (§514)
- Personal representative (§502)



HIPAA Privacy

1. No use/disclosure unless permitted

– Business Associate “types”:

Level 1 - Occasional PHI contact

Level 2 - Regular PHI contact

Level 3 - Possession of PHI

Level 4 - Out-source covered entity’s compliance activities



HIPAA Privacy

1. No use/disclosure unless permitted

– Business Associate

*Suggestion: Work on compliance
from Level 4 to Level 1*



HIPAA Privacy

1. No use/disclosure unless permitted

– Business Associate issues:

- Treatment and workforce excepted
 - What is “workforce”?
- Contract requires restrictions, safeguards, violation reporting, support for patient rights, return/destroy on termination
- CE must require cure of pattern of violations
- If not, termination if feasible or report



HIPAA Privacy

1. No use/disclosure unless permitted

– “Minimum Necessary” (§514)

a. Exceptions

- treatment, patient requests and “required by law”
- New exception – “Incidental Disclosures”

b. Routine uses

- Identify people who need access to PHI
- Identify what PHI they need access to
- Limit their access to the needed PHI

c. Routine disclosures and requests

d. Non-routine uses, disclosures and requests

e. “Entire record requests”



HIPAA Privacy

1. No use/disclosure unless permitted

– “Minimum Necessary” (§514)

Suggestions:

- Start with a general policy
- Implement 1) requests,
2) disclosures, 3) uses



HIPAA Privacy

2. Permitted Uses/Disclosures

- A. For treatment, payment and healthcare operations (formerly “consent”) (§506)
- B. With authorization (§508)
- C. “Opt-opt” situations (§510)
- D. Exceptions (§512)
- E. Patient (§524)



HIPAA Privacy

2. Permitted Uses/Disclosures

- A. For treatment, payment & health care operations (§506)
 - Formerly “consent”
 - Now tied to Notice of Privacy Practices (see §520, below)
 - Still need form under many states’ laws



HIPAA Privacy

2. Permitted Uses/Disclosures

A. For treatment, payment & health care operations (§506)

- What are “health care operations”?
 - Quality improvement
 - Credentialing
 - Underwriting
 - Legal and compliance
 - Planning
 - Management and administration



HIPAA Privacy

2. Permitted Uses/Disclosures

B. With authorizations (§508)

- Specific form
- Generally can't compound or condition
- Right to revoke
- No longer additional requirements



HIPAA Privacy

2. Permitted Uses/Disclosures

B. With authorizations (§508)

“Psychotherapy notes” are:

notes ... by a ... mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual’s medical record.



HIPAA Privacy

2. Permitted Uses/Disclosures

B. With authorizations (§508)

“Psychotherapy notes” exclude:

medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.



HIPAA Privacy

2. Permitted Uses/Disclosures

B. With authorizations (§508)

“Psychotherapy notes”

Suggestion: Develop a separate record system for psychotherapy notes to access these additional rights.



HIPAA Privacy

2. Permitted Uses/Disclosures

B. With authorizations (§508)

- Specific form
- Generally can't compound or condition
- Right to revoke
- No longer additional requirements



HIPAA Privacy

2. Permitted Uses/Disclosures

Strategy:

- Develop a separate record system for psychotherapy notes to access these additional rights.



HIPAA Privacy

2. Permitted Uses/Disclosures

C. "Opt-outs" (§510)

- Directory information
 - Name, location and general condition
 - Religion for pastoral care only
- Involvement in care and notification
 - When the patient is present
 - In the patient's absence



HIPAA Privacy

2. Permitted Uses/Disclosures

D. Exceptions (§512) *(Slide #1)*

- a) required by law
- b) public health activities
 - disease reporting
 - death certificates
- c) victims of abuse, neglect or domestic violence
 - may have to inform the victim
- d) health oversight activities
 - Licensure
 - Not JCAHO



HIPAA Privacy

2. Permitted Uses/Disclosures

D. Exceptions (§512) *(Slide #2)*

- e) judicial and administrative proceedings
- f) law enforcement purposes
 - reporting crimes, injuries, etc.
- g) decedents
 - coroners
- h) organ, eye, tissue donation
- i) research purposes
- j) to avert serious threat to health or safety
- k) specialized government functions
- l) worker's compensation



HIPAA Privacy

2. Permitted Uses/Disclosures

D. Exceptions (§514) *(continued)*

- m) fundraising
- n) underwriting

Note: marketing has been deleted as an exception



HIPAA Privacy

2. Permitted Uses/Disclosures

D. Exceptions

Suggestion: Use the following implementation process:

1. Track all non-TPO disclosures over the next 3 months
2. Identify basis and check preemption
3. Write short policy for each



HIPAA Privacy

2. Permitted Uses/Disclosures

E. Patient (§524)

See next section



HIPAA Privacy

3. Other Patient Rights

A. Notice of privacy protections (§520)

B. Requests for additional protections (§522)

C. Access (inspection and copying) (§524)

D. Amendment (§526)

E. Accounting for disclosures (§528)



HIPAA Privacy

3. Other Patient Rights

A. Notice of privacy protections (§520)

- Right to notice
- Content
 - Uses and disclosures
 - Patient's rights
 - Covered entity's obligations
 - Reserve right to change practices retroactively
- Providing notice
 - Acknowledgement
- Joint notice



HIPAA Privacy

3. Other Patient Rights

A. Notice of privacy protections (§520)

Suggestion:

- 1) Identify state-specific draft early
- 2) Continually re-write during implementation
- 3) Publish last



HIPAA Privacy

3. Other Patient Rights

B. Requests for additional protections (§522)

- Right to request additional restrictions
 - No obligation to comply
- Right to request alternative communication
 - Must accommodate if reasonable



HIPAA Privacy

3. Other Patient Rights

C. Access (§524)

- Right to inspect and copy
- Unreviewable grounds for denial
 - Psychotherapy notes
 - Anticipation of litigation
 - Research
- Reviewable grounds for denial
 - Review process
- Copy charges and timeliness



HIPAA Privacy

3. Other Patient Rights

C. Access (§524)

Suggestion: Identify “health care professional” to perform reviews



HIPAA Privacy

3. Other Patient Rights

D. Amendment (§526)

- Right to offer
- Acceptance
 - Transmittal
- Denial
 - Grounds (accurate & complete, not your record, etc.)
 - Right to submit statement
 - Rebuttal



HIPAA Privacy

3. Other Patient Rights

E. Accounting for disclosures (§528)

- Right to accounting
- Excluded disclosures
 - Almost all
- Content of accounting
 - Date, name, address, description & purpose



HIPAA Privacy

3. Other Patient Rights

E. Accounting for disclosures (§528)

Suggestion: Track all disclosures in chart and produce accounting from that data.



HIPAA Privacy

4. Administrative Requirements (§530)

- privacy officer
- training
- safeguards & security
- complaints to the covered entity
- policies and procedures
- documentation
- sanctions
- verification



HIPAA Privacy

4. Administrative Requirements (§530)

- Privacy officer
 - Responsible for implementation
 - No credentials required by rule
 - Can be shared
 - Can be same as security officer



HIPAA Privacy

4. Administrative Requirements (§530)

– Privacy officer

Suggestions:

- Use HIM director or administrator
- Use job descriptions available on web as starting point



HIPAA Privacy

4. Administrative Requirements (§530)

– Training

- Workforce only
- Trained on policies and procedures
 - Before effective date
 - Upon new hiring
 - When policies and procedures are changed
- No special form required



HIPAA Privacy

4. Administrative Requirements (§530)

– Training

Suggestions:

- Provide general awareness training
- Provide policies and procedures
- Provide periodic in-service training
- Don't just “check it off the list”



HIPAA Privacy

4. Administrative Requirements (§530)

– Safeguards & security

- Both physical and electronic
- Documented security procedures
- “Scalable” to what is “reasonable”



HIPAA Privacy

4. Administrative Requirements (§530) – Safeguards & security

Suggestions:

- Use outside resources for technical issues
- Document what is “reasonable”
- Approach incrementally



HIPAA Privacy

4. Administrative Requirements (§530) – Complaints to the covered entity

- Must designated to receive complaints
- Can be privacy officer
- No particular resolution required
- Must document resolution, if any



HIPAA Privacy

4. Administrative Requirements (§530)

– Complaints to the covered entity

Suggestions:

- Keep a log of complaints
- Use as an opportunity to avoid bigger problems



HIPAA Privacy

4. Administrative Requirements (§530)

– Policies and procedures

- Required for all of the above
- Described in Notice of Privacy Practices
- Changed retroactively only if reserved
- No requirement for specificity



HIPAA Privacy

4. Administrative Requirements (§530)

– Policies and procedures

Suggestions:

- Start with existing policies
- Add any that are missing
- Begin by simply restating the rule
- Modify as practice requires



HIPAA Privacy

4. Administrative Requirements (§530)

– Documentation

- Required for many requirements
- Retention is six years



HIPAA Privacy

4. Administrative Requirements (§530)

– Documentation

Suggestions:

- Incorporate into existing policies
- Keep master list of types and locations



HIPAA Privacy

4. Administrative Requirements (§530)

– Sanctions

- Required for both privacy and security
- No specific type of sanction required



HIPAA Privacy

4. Administrative Requirements (§530)

– Sanctions

Suggestions:

- Be careful with “zero tolerance”
- Consider flexibility
- Address business associate sanctions in BA agreements



HIPAA Privacy

4. Administrative Requirements (§530)

– Verification

- Verify both identity and authority
- Documentation requirements



HIPAA Privacy

4. Administrative Requirements (§530)

- Verification

Suggestion:

- Make part of all training and retraining



HIPAA Privacy

5. Technical Provisions

- Preemption of State Law (160 CFR 201 et seq.)
- Compliance and Enforcement (160 CFR 300 et seq.)
- Transition provisions (§532)



HIPAA Privacy

Proposed Changes

- Published March 27, 2002
- Effective August 14, 2003
- Major provisions
 - Elimination of consent
 - Marketing re-write
 - Changes to notice, accounting and authorizations
 - Extend business associate contracting deadline
 - Many more



HIPAA Privacy

Questions?



HIPAA Overview

Gregory D. Frost
Adams and Reese LLP

451 Florida Street
19th Floor, North Tower
Baton Rouge, Louisiana 70802
225-336-5200
FrostGD@arlaw.com



**Regular teleconferences
on HIPAA privacy
issues**

www.HIPAAEducationNetwork.com



HIPAA Basics for Physicians

**The 123rd Annual Meeting of the
LSMS House of Delegates**

