
HIPAA: Coverage and Implementation Issues (Focus on EDI and Privacy)

Robyn A. Meinhardt, RN, JD

October 16, 2000

First National HIPAA Summit

Washington, D.C.

What This Presentation Will Address

- ◆ New Definitions for Covered Entities
- ◆ Criminal/civil sanctions: for whom, when
- ◆ When do the EDI standards apply? A method for analysis
- ◆ EDI Implementation Problems
- ◆ Issues in Privacy Coverage and Implementation

Citations

- ◆ HIPAA's Administrative Simplification provisions:
 - ◆ 42 U.S.C. 1320d - 1320d-8
- ◆ Standards for Electronic Transactions (final "EDI" rule):
 - ◆ Fed. Reg. Vol. 65, No. 160, August 17, 2000, pp. 50312-50372

Citations, cont'

- ◆ Standards for Privacy of Individually Identifiable Health Information (proposed rule):
 - ◆ Fed. Reg. Vol. 64, No. 212, November 3, 1999, pp. 59918-60065
- ◆ Page numbers in this outline refer to the Federal Register for either the proposed privacy rule or the final EDI rule, according to context, unless otherwise specified.

Health Care Provider, Defined:

- ◆ By the statute (42 U.S.C. 1320d(3):
 - ◆ “includes a provider of services (as defined in section 1861(u) [Medicare Part A [organizational] providers]), a provider of medical or other health services (as defined in section 1861(s) [Medicare Part B [physicians, certain other licensed individual providers, those who supply medical devices and supplies]]), and any other person furnishing health care services or supplies.”
- ◆ By the proposed Privacy rule (p. 59930): “includes many types of therapists, technicians and aides.”

Health Care Provider, Defined:

- ◆ By the proposed Standard Health Care Provider Identifiers rule (Fed. Reg. Vol. 63, No. 88, May 7, 1998, p. 25325-26): includes individual, group and organizational health care providers “who bill and are paid for health care services or supplies.”
 - ◆ “Individuals” would NOT include “health industry workers who support the provision of health care but who do not provide health services, such as admissions and billing personnel, housekeeping staff, and orderlies.”
 - ◆ “Organizations” would include physician group practices.

Health Plans, Defined:

- ◆ By the statute: “an individual or group health plan that provides, or pays the cost of, medical care” (42 U.S.C. 1320d(5).)

Includes:

- ◆ employee welfare benefit plans/any other arrangement for health benefits to employees of 2 or more employers
- ◆ ERISA plans that either (a) have at least 50 participants or (b) are under a third party administrator

Health Plans, Redefined:

- ◆ By the final EDI rule: the statute and previous definitions referred to two types of health care coverage policies (a policy for long term care, and Medicare supplemental policies) as “health plans.” The EDI rule clarifies that it is the issuer of those policies (not the policies themselves) that are “health plans” subject to HIPAA’s rules (p. 50321).

Health Care Clearinghouses, Clarified:

- ◆ By the statute: “a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.” (42 U.S.C. 1320d(2).)
- ◆ The final EDI rule clarifies that regulatory references to billing services and repricing companies are not alone sufficient to bring them into the clearinghouse definition (p. 50319).

Who Pays? Who Goes to Jail?

Civil and Criminal Penalties

- ◆ Civil penalties: \$100/“provision,” up to \$25,000 annually per “provision”
 - ◆ “knew or should have known” standard
 - ◆ don’t apply:
 - ◆ when noncompliance due to “reasonable cause,” no willful neglect AND compliance corrected within 30 days of discovery/should have discovered the violation
 - ◆ to criminal offenses

Criminal Penalties

- ◆ Apply when HIPAA is violated by:
 - ◆ obtaining or disclosing identifiable health information, or
 - ◆ using, or causing the use of, a unique health identifier (allowed uses still to be defined)
- ◆ Must be “knowingly and in violation” (in contrast to “knowingly in violation”)

Criminal Penalties

- ◆ Knowingly and in violation: \$50,000/1 year
- ◆ Under “false pretenses”: \$100,000/5 years
- ◆ With intent to sell, transfer or use for “personal gain/commercial advantage/malicious harm”: \$250,000/10 years

Civil and Criminal Penalties Apply Only to Covered Entities

- ◆ Criminal penalties apply to “[a] person who knowingly and in violation of this part . . .” (42 U.S.C. 1320d-6(a));
- ◆ civil penalties apply to “any person who violates a provision of this part” (42 U.S.C.1320d-5(a)(1);
- ◆ “this part” is “Part C -- Administrative Simplification” of 42 U.S.C. 1301;

Civil and Criminal Penalties Apply Only to Covered Entities

- ◆ the Administrative Simplification provisions of HIPAA apply only to health care providers, health plans and health care clearinghouses;
- ◆ **therefore, only a covered entity can violate “this part.”**

Selected Issues in EDI Coverage: Applicability to Health Care Providers

- ◆ Proposed: rules applied to a health care provider “when transmitting” a transaction electronically
- ◆ Final: rules apply to a health care provider “who transmits any health information in electronic form in connection with a transaction” -- i.e., reverted to statutory language
- ◆ But examples allow HCP to use both paper and electronic transactions (p. 50314), so apparently rules apply only “when transmitting” electronically

Selected Issues in EDI Coverage: Applicability to Specific Technologies

- ◆ Proposed: rules wouldn't apply to telephone voice response, fax-back and Hyper-Text Markup Language (HTML, for Internet websites)
- ◆ Final rule: There are “certain transmission modes” where standard formats would be “inappropriate,” but only “direct data entry” by health care provider into health plan's computer is exempted from format (not from data content requirements). (p. 50315)

Selected Issues in EDI Coverage: Application to Transactions

- ◆ Step 1: Identify parties to the transaction and compare to definition
- ◆ Example 1: Health Plan contracts with TPAs and data service company (“DataCo”); TPAs and DataCo exchange eligibility inquiries/responses.
- ◆ Note: Business associates of a covered entity are deemed to act for that entity.

EDI Application to Transactions, cont'

- ◆ Analysis:
 - ◆ Parties: TPAs and DataCo are all deemed to be acting as Health Plan
 - ◆ Eligibility Inquiry Transaction (Section 162.1201(a)) defined as either:
 - ◆ between health plan and HCP, or
 - ◆ between two health plans
- ◆ Result: **RULES DO NOT APPLY** because there are no separate parties involved

EDI Application to Transactions, cont'

- ◆ Example 2: HP submits monthly bill to State Medicaid agency for capitation payment, as per contract.
- ◆ Analysis:
 - ◆ Parties are each covered entities (health plans)
 - ◆ A Health Care Claims/Equivalent Encounter Information Transaction (Section 162.1101) is the transmission of either:

EDI Application to Transactions, Example 2, cont'

- ◆ a request to obtain payment, with necessary accompanying information, from HCP to health plan, for health care, or
- ◆ if there is no direct claim [such as with capitation payments], encounter information for the purpose of reporting health care.
- ◆ **Result: RULES DO NOT APPLY** because this transaction is between two health plans, while the definition requires the payment request to be from an HCP to a health plan.

EDI Application to Transactions, Example 3

- ◆ Example 3: After the payment request in Example 2 is made, the State Medicaid program pays the health plan.
- ◆ Analysis: A Health Care Payment and Remittance Advice Transaction (Section 162.1601) includes the transmission of payment from HP to HCP.
- ◆ This standard doesn't apply: transaction involves two health plans

EDI Application to Transactions, Example 3, cont'

- ◆ BUT: a Health Plan Premium Payment Transaction (Section 162.1701) includes transmission of payment “from the entity that is arranging for the provision of health care *or is providing health care coverage payments for an individual to a health plan,*” as is the State Medicaid program.
- ◆ Result: Transaction must comply with the transaction standards.

“We acknowledge that the coding systems proposed as initial standards may not address all business needs,” such as the ability to submit claims for certain services such as:

- ◆ alternative health care procedures;
- ◆ home infusion;
- ◆ dental diagnoses;
- ◆ mental health functional status;
- ◆ behavioral health;
- ◆ chronic conditions and functional status covered by long term care policies

EDI Implementation Problems: Inadequate Codes

- ◆ Solutions proposed by DHHS to inadequate codes:
 - ◆ manual processing
 - ◆ submit modification requests to Designated Standards Maintenance Organizations
- ◆ Concern that national standard setting process is too slow to timely develop codes for new technologies. DHHS: use NOS code (Not Otherwise Specified)

EDI Implementation Problems: Timing/Coordination

- ◆ DHHS sanguine about industry coordination/adequate implementation time (see pp. 50328, 50335, 50346, 50353)
- ◆ They “encourage health plans not to require health care providers to use standards . . . during the first year” of the implementation period, and “to give health care providers at least 6 months notice” before requiring use of a standardized transaction. (p. 50321).

EDI Implementation Problems: Timing/Coordination, cont'

- ◆ Note: New Jersey is requiring HIPAA compliance in 12, rather than 26, months.
- ◆ Concerns exist over costs of maintaining duplicate systems during implementation, but DHHS expects health plans to routinely maintain earlier versions of medical code sets, to allow for late resubmissions of medical data (p. 50323).

EDI: Regulations Still to Come

- ◆ Preemption rules to be issued for EDI “when the preemption issues have been resolved in the context of privacy” (p. 50318).
- ◆ Enforcement regulations, which are to be in effect when other regulations become enforceable (no 26-month wait) (p. 50334).
- ◆ Health Care Provider definition issues to be resolved by final rules for HCP Identifier
- ◆ Health claims attachments, other identifiers

EDI Implementation: Correlation to Privacy

- ◆ DHHS encouraging collection of demographic data for research (p. 50337)
- ◆ EDI rules to be delayed until privacy rules in force

Privacy Implementation: “Protected Health Information”

- ◆ PHI is:
 - ◆ “related to an individual’s health or medical condition,” and
 - ◆ has been put into electronic format (“computer” involved)
 - ◆ by any covered entity
 - ◆ at any time
 - ◆ whether you know about it or not
- ◆ **Information** protected - not documents

Privacy Implementation: Identifying PHI

- ◆ “Electronic format” requirement is irrelevant as to PHI, because:
 - ◆ impossible to know that electronic format has NOT been used
 - ◆ impossible to administer two sets of confidentiality policies, one for PHI and one for solely paper-based information
 - ◆ impossible to avoid mixing PHI and solely paper-based information

Privacy Implementation: Rules for Disclosure

- ◆ Prohibited unless expressly allowed
- ◆ Allowed for:
 - ◆ treatment, payment, health care operations and sometimes research
 - ◆ specified public health and other government-requested disclosures
 - ◆ when authorized by the patient

Privacy Implementation: Research Issues

- ◆ Disclosure of “research information unrelated to treatment” requires individual authorization, OR
- ◆ Use/disclosure without authorization requires IRB/privacy board findings:
 - ◆ that PHI is necessary to the research project
 - ◆ that specified protections for PHI are in place
- ◆ Use of “de-identified information” constrained by strict definition

Privacy Implementation: When Authorization is Required for “Operations” Disclosures

- ◆ Individual authorization required:
 - ◆ When not otherwise allowed by the regulations
 - ◆ Even when allowed as an “operations” disclosure, for:
 - ◆ **marketing of health and non-health items and services** (Ex.: CVS/Elensys (Adheris))
 - ◆ **disclosure by sale, rental or barter**
 - ◆ **to non-health divisions** of a company

Privacy Implementation:

Disclosures with Financial Benefit

- ◆ “Financial Benefit” Rule for requesting individual authorization:
 - ◆ Determine whether “financial or in-kind compensation” will result to the covered entity
 - ◆ If so, the authorization form signed by the patient must so state
- ◆ Noncompliance with the “financial benefit rule” invokes HIPAA’s strictest penalties
 - ◆ up to \$250,000 fine and 10 years jail

Privacy Implementation: Disclosures with Financial Benefit

- ◆ What if community health activities are “marketing”?
 - ◆ disease management
 - ◆ community educational efforts
 - ◆ **individual authorization required**
 - ◆ severest sanctions: 10 years/\$250,000

Privacy Implementation: Minimum Necessary

- ◆ Only the minimum necessary PHI may be disclosed, as measured by the purpose of the disclosure
- ◆ Applies to internal as well as external disclosures
 - ◆ For treatment, operations, payment
 - ◆ Opposite of IOM Report recommendations

Privacy Implementation: Contracts with Business Partners

- ◆ Chain of trust/business partners/business associates/trading partner agreements
- ◆ derivative confidentiality obligations:
 - ◆ for other covered entities
 - ◆ for non-covered entities
- ◆ “third party beneficiary” clause: now or later?
- ◆ obligation to monitor?

Privacy Implementation: Patients' Rights

- ◆ To request more protections
 - ◆ Define enforcement or prohibit
- ◆ To inspect and copy health information
- ◆ To request amendment of health information
 - ◆ “Amendments” versus “addenda”

Privacy Implementation: Patients' Rights

- ◆ To receive “accounting” of disclosures
 - ◆ audit trails: human-readable; reviewed
- ◆ To receive notice of information practices
 - ◆ Compare sample notice (p. 60049) to stated requirements (pp. 59976-78)
 - ◆ Doesn't apply to HCCs, business partners

Privacy Implementation: Administrative Changes

- ◆ Privacy official/complaint processor
- ◆ Mitigate harm when PHI wrongly disclosed
- ◆ Personnel training in confidentiality practices (HIPAA is 80% procedural/personnel, 20% technological)
- ◆ Compliance documentation

Privacy Implementation: Preemption

- ◆ State laws not preempted if:
 - ◆ contrary to and more stringent than federal rules
 - ◆ public health reporting laws
 - ◆ health plan reporting requirements
 - ◆ the Secretary determines they're necessary

Privacy Implementation: Preemption

- ◆ “More stringent” means:
 - ◆ less disclosure of information
 - ◆ more personal access
 - ◆ greater penalties
 - ◆ greater disclosure of privacy practices
 - ◆ more onerous authorization requirements
 - ◆ enhanced accounting and retention

Privacy Implementation: Preemption

- ◆ State law preemption a moving target
- ◆ A morass of conflicting determinations
- ◆ No preemption authority
- ◆ No clarity for covered entities
- ◆ Significant civil liability exposure and opportunity for criminal penalties

Questions?

Robyn A. Meinhardt, RN, JD

Foley & Lardner

1999 Broadway, Suite 2560

Denver, CO 80202

303-294-4414

rmeinhardt@foleylaw.com