Banks and the Privacy of Medical Information

8th National HIPAA Summit
March 8, 2004

Joy Pritts, JD
Health Policy Institute
Georgetown University
202-687-0880
Public Concerns

95% adult Americans do not want banks to have access to their medical record information without their permission.*

Information Networks: HIPAA & GLBA

Protected Health Info. (PHI)

Health Care Provider

Banks

Health Plan

Joy Pritts, JD
Public Concerns

Increased access to identifiable health information by banks
+ Increase in bank-insurer affiliations
+ More sophisticated computer technology
+ Potential financial incentive

Concerns about banks obtaining and using health information for consumer credit decisions & sharing health information with affiliates
Goal: Protect Privacy of Health Info. as It Flows through the System

Claim for payment

Protected Health Info.

Health Plan

Health Care Provider

Banks

Covered

Covered

Joy Pritts, JD
Primary Laws

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Gramm-Leach-Bliley Act (Financial Services Modernization Act) 1999
- Fair and Accurate Credit Transactions Act of 2003 (FACT Act)
  - Amendments to Fair Credit Reporting Act
HIPAA & Banks

Are banks covered by HIPAA?
What activities of banks, if any, make them “health care clearinghouses” covered by HIPAA?
Processing Consumer Payment Info. Does *Not* Make a Bank a HIPAA Clearinghouse

Joy Pritts, JD

Covered

Health Care Provider

Checks or Credit Card Payments

Patient

3d Party or Affiliates

Bank

Credit Card Co.

NOT Covered

Info.
Processing 3d Party EFT Does Not Make a Bank a HIPAA Clearinghouse

EFT

Bank

EFT

Bank

Covered

Health Care Provider

Claim for payment

Covered

Health Plan

Joy Pritts, JD
Does Processing ERAs Make a Bank a HIPAA Clearinghouse?

CLAIM FOR PAYMENT

ERA – IDENTIFIABLE HEALTH INFO.

NOT COVERED – Sec. 1179 Exemption?

Covered

Health Care Provider

Bank

ERA

Bank

Info.

3rd Party or Affiliate

Covered

Health Plan

Claim for payment

Joy Pritts, JD
Sec. 1179

PROCESSING PAYMENT TRANSACTIONS BY FINANCIAL INSTITUTIONS

SEC. 1179. To the extent that an entity is engaged in activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following:

(1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check or electronic funds transfer.

* * *

42 USCS § 1320d-8

Joy Pritts, JD
Issue

If banks are exempt from HIPAA under 1179, to what extent is medical information held by banks protected by other laws?
GLBA

- Designed to encourage affiliations between banks and other “financial institutions”

- Applies only to consumer & customer financial information, not commercial transactions

- Privacy provisions establish limits on sharing financial information (which may contain medical info.)
GLBA Limits *Sharing* Consumer Payment Info.

- **Covered Bank**
  - Notice & Opt Out Information
  - Checks or Credit Card Payments

- **3d Party**
- **Patient**
- **Affiliates**
- **Health Care Provider**

Joy Pritts, JD
GLBA Does *Not* Prohibit Banks from *Using* Consumer Payment Info.

- **Covered**
  - Health Care Provider
  - Patient
  - Checks or Credit Card Payments

- **NOT Covered**
  - Bank
  - Credit Card Co.
  - Checks or Credit Card Payments
GLBA Doe *Not* Prohibit Banks from *Using* or *Sharing* Info. from *Commercial* Transactions

3d Party

Bank

ERA

Not Covered by GLBA

Health Care Provider

Claim for payment

Health Plan

Joy Pritts, JD

Affiliates

ERA – Identifiable Health Info.
Intent of FACT Act

Fill some of gaps in privacy protections in:

- HIPAA
- GLBA
- Within context of consumer credit protections
FACT Act

- Prohibits obtaining & using medical information for *consumer credit decision* purposes except where banking agencies determine it is “necessary and appropriate” to protect legitimate operational, transactional, risk, consumer and other needs.

- Consistent with intent to restrict use of medical info. for inappropriate purposes.
Regulations Drafted by Banking Agencies that Allow Using Info. for Credit May be Narrow...
... or Broad

Covered

Banks

Claim for payment

ERA – Identifiable Health Info.

EFT

Health Care Provider

Health Plan

Joy Pritts, JD
FACT Act Does *Not* Prohibit *Using* Payment Info. for Insurance, Marketing or Other Purposes
Limits on Sharing Medical Info. Are Not Clear

Under best circumstances, permits banks to share medical info. with affiliates for any purpose:

- Permitted without authorization under Privacy Rule or
- Referred to under Section 1179
Conclusion

If banks are fully exempt under Sec. 1179, the medical information that they receive is not fully protected by other laws.
The End