Privacy Rights: The Patient's Perspective

Robert Gellman
Privacy and Information Policy Consultant
Washington, DC
202-543-7923
rgellman@cais.com

Prepared for the Third National HIPAA Summit
Washington, DC
October 26, 2001

Outline

- **Health Data Flows Today**
- **Institutional Response to Privacy**
- **What HIPAA Does and Doesn’t**

Data Flows: Level I

1. Patient visits Doctor with sore throat.

2. Doctor sends culture to Laboratory.

3. Doctor phones prescription to Pharmacy.

Data Flows: Level II

4. Pharmacy sends prescription data to Pharmacy Benefit Manager.

5. Doctor/Laboratory send bill to Clearinghouses.

6. Clearinghouses send bill to Payor.

7. Payor may share data with Employer.

Data Flows: Level III

8. PBM may share data with Marketer.
9. STD? Notify Public Health.
10. Birth Defect? Notify Registry.
11. Knife Wound? Notify Police.
12. Abuse? Notify Social Service Agency.
13. Complication? Peer Review.
14. Audit? Inspector General.
15. Subpoena? Give records to Anyone.
16. Research Interest? Records to Researchers.
17. Licensing and Accreditation uses.

Data Flows: Level IV

Most recipients share records with:

a. Staff
b. Lawyers
c. Accountants
d. Service Providers (e.g., computers)
e. Managers
f. Overseers and Regulators
g. Inspectors General
h. Police

Data Flows: Level V

Hippocratic Oath

- **Doctor**
- **Pharmacist**

No Oath

- **Lab**
- **PBM**
- **Clearinghouse**
- **Payor**
- **Employer**
- **Researcher**
- **Public Health Dept.**
- **Inspector General**
- **Welfare Agency**
- **Police**

Conclusion I

Of all personal records maintained by third party record keepers, medical records are the most widely shared of all.

Compare with bank, marketing, schools, employment, insurance, credit, motor vehicle, library, telephone, cable television, video rental, etc.

Conclusion II

- **Medical records are not confidential.**
- **Patients think records are confidential.**
- **No one wants to tell patients the truth.**
- **Most people with access have no relationship with patient.**

Institutional Negligence I

What does your doctor, hospital, pharmacy tell you about data use, privacy or patient rights?

Patient “consent” forms

Health plan policy small print

Institutional Negligence II

Privacy Training?
Privacy Office?
Written privacy policy?
Privacy Audits?
List of laws regulating records?

Health Care Institutions have ignored their privacy obligations for years.

What HIPAA Does

A *Covered Entity* must

- **have a written privacy policy**
- **inform patients of their rights**
- **limit use and disclosure of records**
- **pay attention to its service providers**
- **be accountable**

Patient get notice and a few rights.

Employers must limit use of health data.

What HIPAA Doesn't

- **Give patients real control over records**
- **Limit any existing use or disclosure**
- **Restrict police access or use (but see EO 13181)**
- **Regulate all health record keepers**
- **Apply to most Internet websites**
- **Stop marketing uses of patient data**