Health Information Privacy and Confidentiality

Lawrence O. Gostin, J.D., LL.D. (Hon.)
Professor of Law, Georgetown University;
Professor of Public Health, Johns Hopkins University;
Director, Center for Law & the Public's Health

National Health Information Infrastructure 2003:
Developing a National Action Agenda for NHII
July 1, 2003

Institute of Medicine on the National Health Information Infrastructure

- “No one engaged in any of the health care delivery or planning today can fail to sense the immense changes on the horizon, even if the silhouette of those changes, let alone the details, are in dispute.”

- *See* Institute of Medicine, *

Definitions

- National Health Information Infrastructure – the basic, underlying framework of electronic information collection, storage, use, and transmission that support all of the essential functions of the system.
- Health Information Privacy – individuals claim to control the circumstances in which personally identifiable data are collected, used, and transmitted.
- Security – technological, organizational, and administrative safety practices, policies, and procedures designed to protect data systems against unwarranted disclosure, modification, or distribution and to safeguard the system itself (e.g., encryption, sign-on security codes, audit trails). Secure data systems keep health records safe from unauthorized use.

Security ≠ Privacy

- 1) Even with 100% security there is not complete privacy. Authorized users can access data.
- 2) No security measures can prevent invasion of privacy by those who have authorization to access records.

- *See* Lawrence O. Gostin, *Personal Privacy in the Health Care System: Employer-Sponsored Insurance, Managed Care, and Integrated Delivery Systems*, 7 Kennedy Institute of Ethics Journal 361-376 (1997).

Tradeoffs

- Privacy – Individual control of personal information
- Public goods - Uses of information:
  - Informed consumer choice
  - Clinical practices
  - Quality assurance
  - Monitor fraud and abuse
  - Track and evaluate utilization and access to health care services
  - Research – determinants, prevention, Rx, health services
  - Cost
  - Public health – surveillance, epidemiological investigations, population-based interventions

National Health Information Infrastructure

- Electronic Longitudinal Patient Records
- Disease, Medical Record, and Genetic Databases
- Unique Identifiers
- Electronic card technology
- Internal (Intranet) and Public (Internet) Networks

- *See* Lawrence O. Gostin, *Health Information Privacy*, 80 Cornell Law Review 451-528 (1995).

Privacy Risks

- Authorized users – systematic flows of data between users in organization, delivery, and financing of health care
  - Lines blurred between employer, payor, provider
  - Data may flow horizontally and vertically between employers, insurers, providers, labs, pharmacies, hospitals, and other health service providers.
  - Secondary uses of data for research, government regulation and oversight, public health
- Unauthorized users
  - Commercial ventures
- Fraudulent/Unlawful users

Ethical Values

- Respect for persons – Autonomy
- Trusting relationships
- Economic harms
- Public health – encourages disclosures
- *See* Lawrence O. Gostin, *Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations*, 127 Annals of Internal Medicine 683-690 (1997).

Health Privacy Law

- Constitutional right to privacy
  - *Whalen v. Roe* grants a limited right to health information privacy.
- Federal law
  - HIPAA Privacy Rules
  - Privacy Act 1974
  - FOIA
- State law
  - Disease specific
  - Extra confidentiality for certain conditions
- Tort

- *See* Lawrence O. Gostin, *Health Information Privacy*, 80 Cornell Law Review 451-528 (1995); Lawrence O. Gostin et al., *The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy*, 275 JAMA 1921-1927 (1996).

Theory Problems in Law and Ethics

- Relationships
  - Ethics: Hippocratic Oath, Trusting relationships between physician and patient
  - Law: Torts
- “Holder” of Data
  - Ethics: Duty on holder to protect data
  - Law: Penalty on holder for unauthorized disclosure of data
- These theories are outdated, but important

CDC – Model Privacy Statute

- Data collection justification
- Data protection review
- Fair information practices
- Information for patients
- Privacy and security assurances
- Secondary uses of data
- Concentric circles of data use

- *See* Lawrence O. Gostin et al., *Informational Privacy and the Public's Health: The Model State Public Health Privacy Act*, 91 American Journal of Public Health 1388 (2001).

HIPAA Privacy Rule

- Only protects certain health information
- Important issues:
  - How to provide privacy outside of HIPAA (e.g. to non-health care entities)
  - Research
  - Public health activities (e.g., surveillance, outbreak investigations)

- *See* Lawrence O. Gostin, *National Health Information Privacy: Regulations Under the Health Insurance Portability and Accountability Act*, 285 JAMA 3015-3021 (2001).

Ethical Issues during Public Health Emergencies

- Do the ethical calculations change during public health emergencies?
- Bioterrorism and emerging infectious diseases (e.g., SARS)
  - Syndromic surveillance
  - Sharing of information with law enforcement, public health, emergency management

- *See, e.g.*, Lawrence O. Gostin, *Public Health Law in an Age of Terrorism: Rethinking Individual Rights and Common Goods*, 21 Health Affairs 79-93; Lawrence O. Gostin et al., *The Model State Emergency Health Powers Act*, 288 JAMA 622-628 (2002) ; Lawrence O. Gostin, *When Terrorism Threatens Health: How Far are Limitations on Personal and Economic Liberties Justified?* __ Florida Law Review __ (2003).

Reconceptualizing Personal Privacy versus Common Goods

- Incorrect assumption that we can have it both ways. There are no easy choices and difficult tradeoffs must be made.
- Two respective claims:
  - Privacy – autonomy is a trump to other interests
  - Public goods – just as salient
- Need closer examination of the nature and power of these two respective claims.

- *See* Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 Minnesota Law Review 1439-1479 (2002).

Reconceptualizing Personal Privacy versus Common Goods

- Privacy
  - Take seriously, but don't assume any privacy claim deserves absolute protection
- Common Goods
  - Do not assume any claim of public good should prevail over privacy
- Balancing allows for
  - Maximizing of privacy where it matters most
  - Maximizing public interests where they matter most

Consider three cases

- Privacy interests strong, public interests weak
  - Disclosure to family, friends, insurer, employer
  - Informed consent is key
- Public interests strong
  - Research
  - Public health
  - Assuming:
    - Legitimate purpose
    - No other way to achieve purpose
    - Privacy and security safeguards
- Hard case
  - Law enforcement
  - Emergency services

Take Privacy Seriously

- Fair information practices
  - Access to own records
  - Corrections of inaccuracies
- Privacy policy
- Security policy
- Nondisclosure rules
- Use of anonymized and linkable data

The Future of Health Information Privacy

- Privacy is inherent in American History and Constitutional Law
- Public goods are a part of the classic republican traditions of America
- Maximizing each of these values will lead to the most vibrant future for health in America: in a democracy, under the rule of law, and with respect for persons and populations.

Other resources

- The Center for Law and the Public's Health www.publichealthlaw.net

- Lawrence O. Gostin, Public Health Law: Power, Duty, Restraint (2000).
- Lawrence O. Gostin, Public Health Law: A Reader (2002).