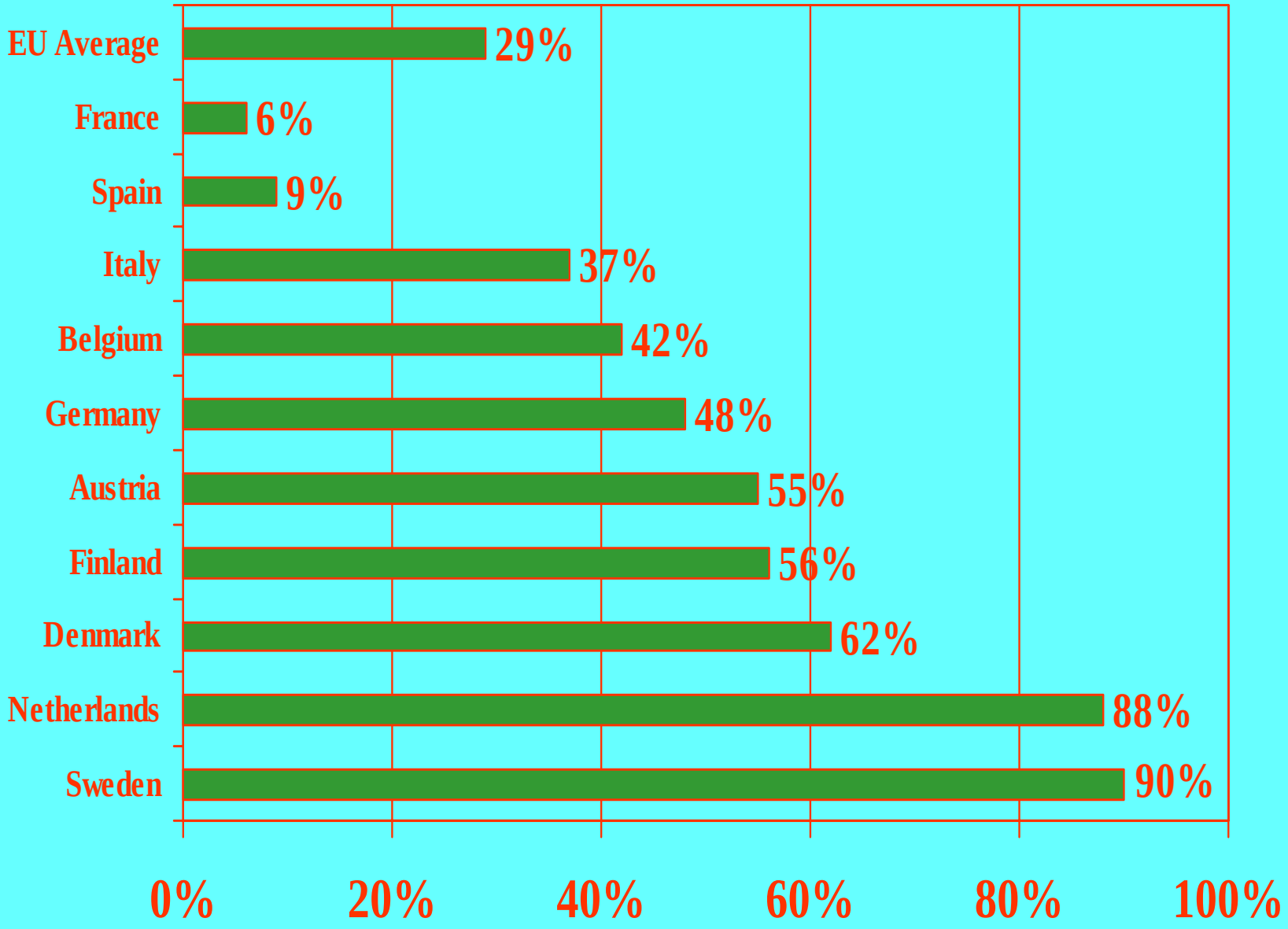
CERIAS Symposium 2007
Transitions:
Paper is to Online as Privacy is to ????

James G. Anderson, Ph.D.

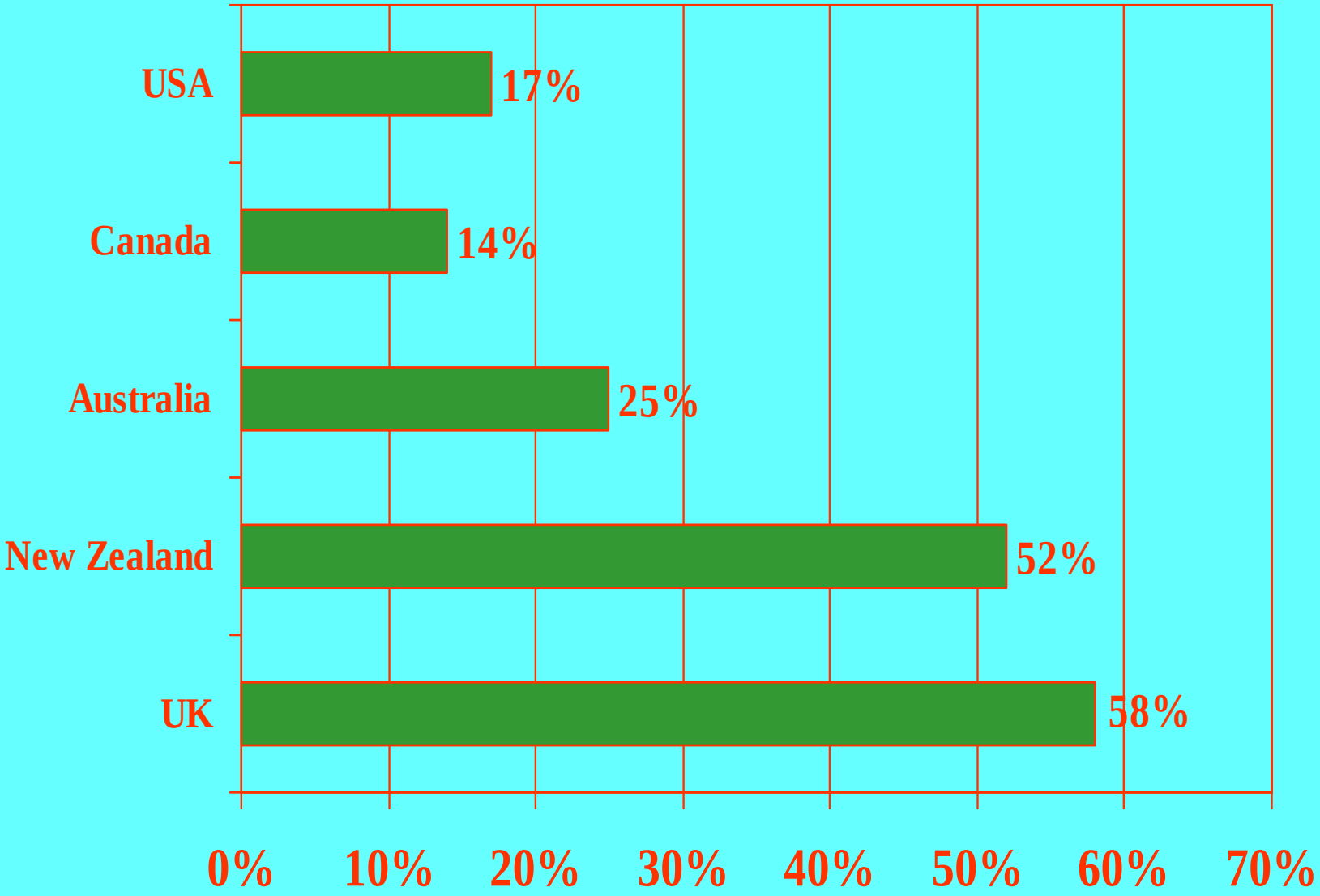
Purdue University

Authorized Users

General Practitioners' Use of EMRs



General Practitioners' Use of EMRs



PROFESSIONAL ETHICS

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself."

Hippocratic Oath

ACCESS TO A PATIENT'S MEDICAL RECORD

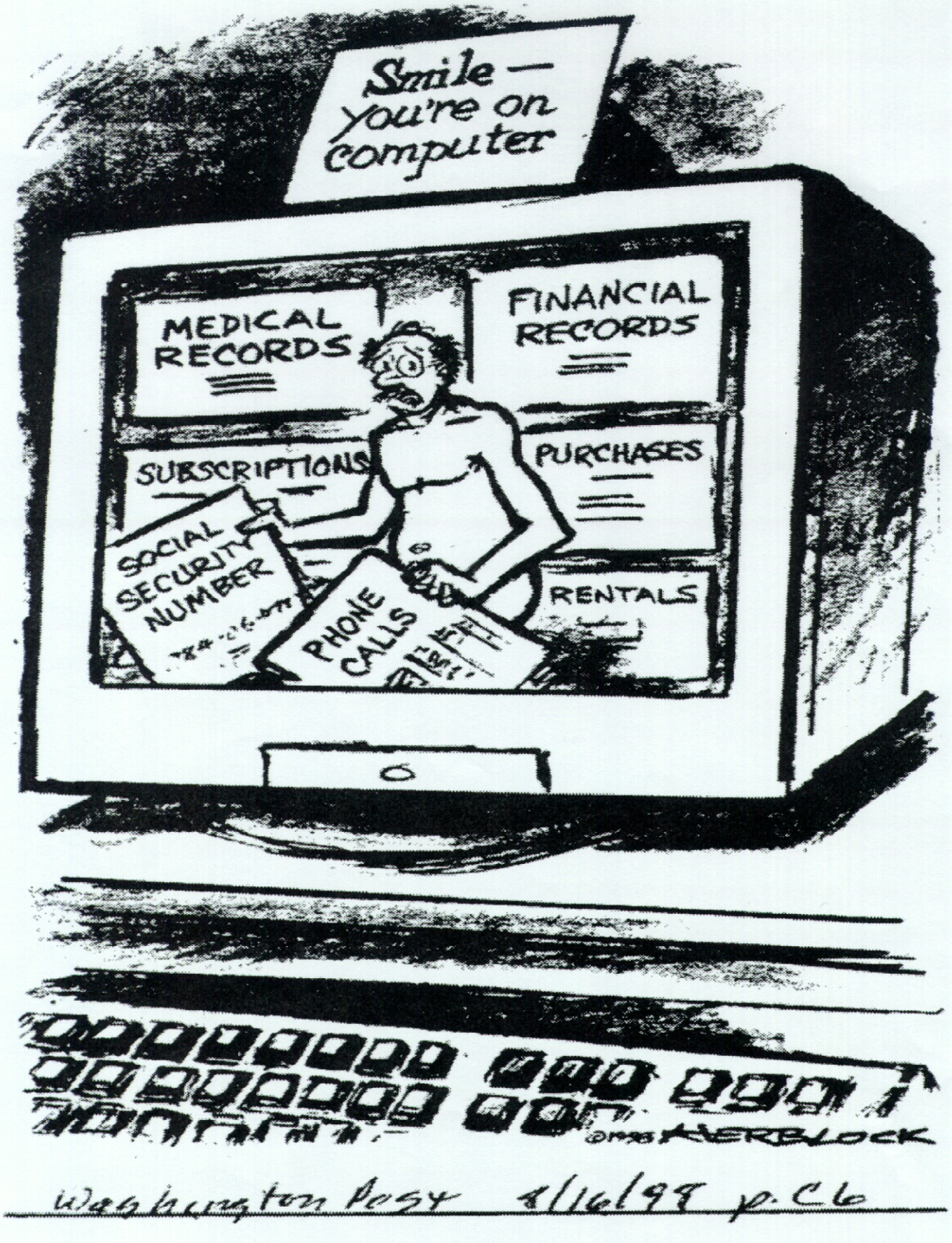
- 6 Attending Physicians
- 12 Residents
- 20 Nursing Personnel
- 6 Respiratory Therapists
- 3 Nutritionists
- 2 Clinical Pharmacists
- 15 Students (medicine, nursing, allied health)
- 4 Ward Clerks
- 4 Hospital Financial Officers
- 4 Medical Chart Reviewers
- 76 TOTAL

ACCESS TO A PATIENT'S MEDICAL RECORD

- Physical Therapist
- Occupational Therapist
- Chaplain
- Social Worker
- Insurance Company
- Employer

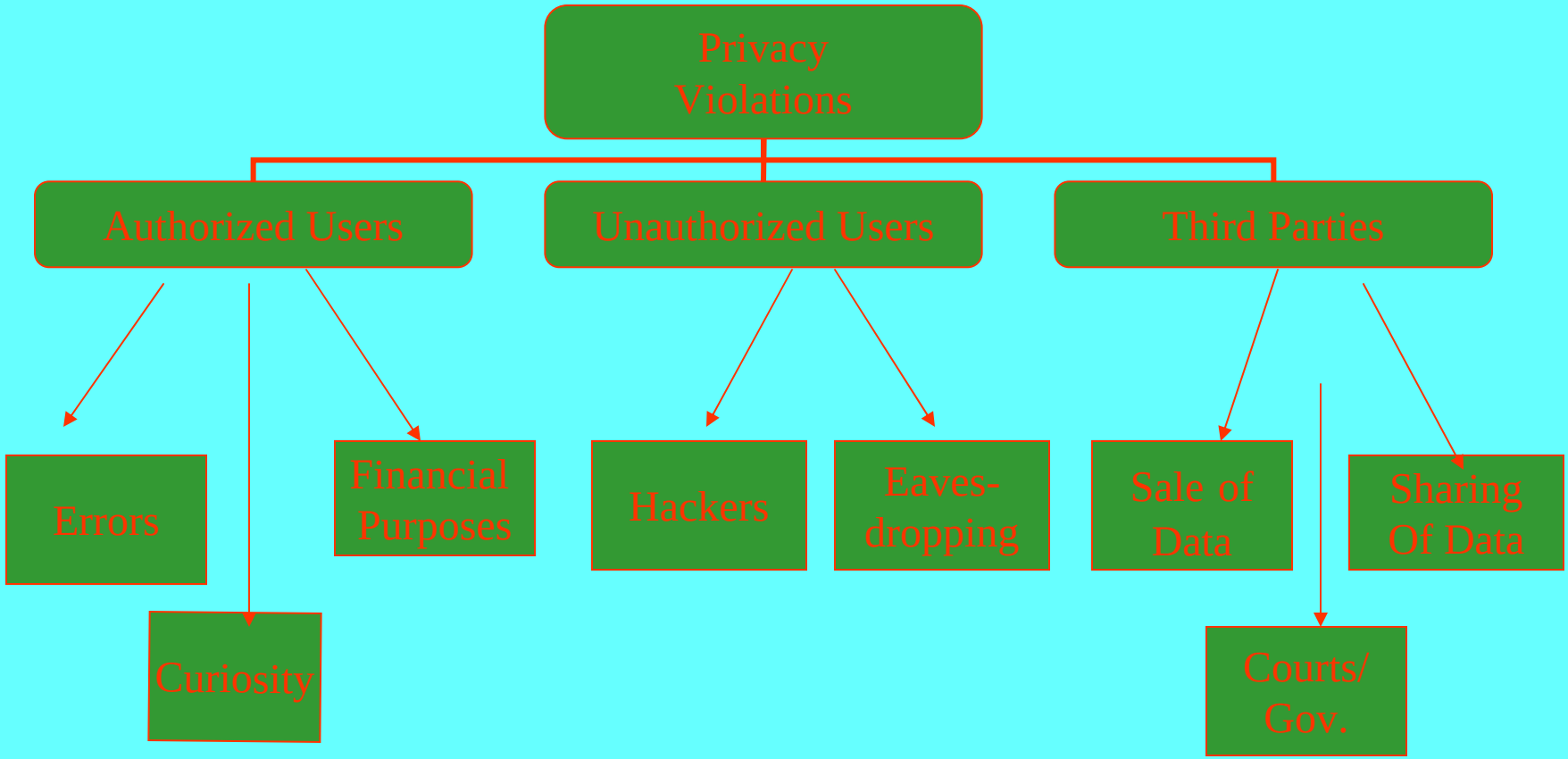
Dilemma

How can we provide data required by the health care industry and at the same time protect the privacy of patients?



Washington Post 8/16/98 p. C6

Threats to Privacy



Threats from Authorized Users

- Errors
- Curiosity
- Financial reasons
- Personal reasons

Privacy and Confidentiality Breach of Security

- A certified sex therapist operated a Web site to treat people for sexual problems. Treatment is conducted over the Internet. In March 1999 the sexual and medical histories of 15 women and 75 men who had consulted the doctor were inadvertently posted on a public Web site.

Illustration by Dave Harbaugh

"He's not learning to play the harmonica . . . It's just confidential when he discusses the patient's medication on his cell phone."

Inappropriate Access to a Celebrity's Medical Records

- The medical team caring for a local celebrity became concerned about the large number of staff members who had accessed the patient's electronic medical record. An audit trail revealed that about 50 individuals not involved in the patient's care had accessed the medical record.

Case Personal Reasons

- A banker who served on a state health commission had access to a computer registry of cancer patients in the state. He called in the loans that his bank had made to all of the patients whose names were included in the registry.

Unauthorized Use of Medical Information

- Fraud
- Personal Use
- Hackers

Credit Card Fraud

- A computer programmer who worked for a physician group practice had access to patient files that contained personal information including credit card numbers. The sheriff's department notified the physician group that their employee had used patients' credit card numbers into purchase items over the Internet.

Case Financial Reasons

- The London Sunday Times reported that detailed medical records for any individual in the U.K. could be purchased for a fee of 150 pounds Private investigators advertised that with the name, address and date of birth of an individual they could provide a summary of anybody's medical records within three hours.

Hackers

- Hackers broke into a computer at a university medical school and used it to generate a flood of e-mail advertisements. The break-in was not discovered for a couple of weeks. A university spokesperson said that no patient files were improperly accessed. Efforts by the university to cope with the intrusion have caused intermittent problems with e-mail service ever since the break-in.

Secondary Uses of Health Information

- Employers
- Insurance companies
- Sale of information to third parties

Case Employers

- Mr F worked for Adolph Coors Co. The company sponsors a wellness center where employees can work out, visit a medical clinic and attend health promotion classes. To qualify for use of the center employees complete a health hazard appraisal form. In 1992 Mr. F died of a heart attack and his widow filed for survivor's benefits and claimed her husband's death was due to job-related causes. The company used information about Mr. F's smoking to persuade an administrative judge to deny his widow benefits.

Third Parties

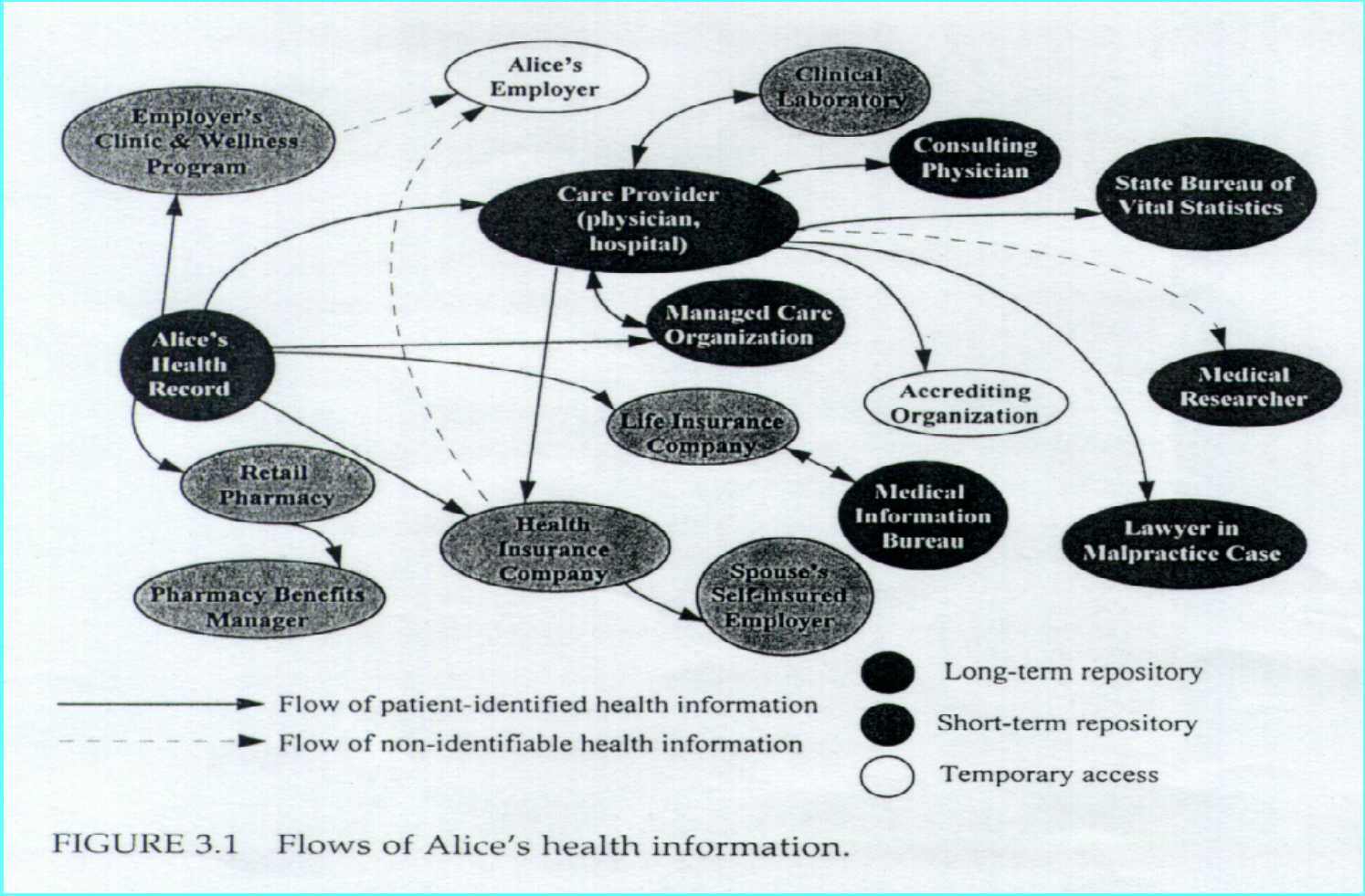


FIGURE 3.1 Flows of Alice's health information.

Use of Web Bugs

- HomeConnection, an Internet Service Provider, has devised an innovative promotion to help increase its subscriber base. The company encourages users with their own personal Web pages to carry an ad for HomeConnection offering new subscribers a discounted rate. The company pays users $25 for each new member signed. When users placed the ad on their Web pages they unknowingly would also get a Web bug that transmitted information to a major on-line ad agency.

Case Sale of Medical Information

- CVS Corporation and Giant Foods sold confidential prescription information, names, addresses and personal information to Elensys Inc. Elensys arranged for drug manufactures to pay pharmacies for the right to send educational material to customers who had specific medical conditions promoting their drugs.

Sale of Consumer Lists

- Toysmart.com operated an on-line toy retail sale In May 2000, it ceased to operate and declared bankruptcy. The company had collected considerable personal data about customers and their children. In spite of stated privacy policies and the TRUSTe seal or trustmark, the company put its customer list up for bids along with the rest of their assets. The company was promptly sued by the FTC since it had broken its promise of confidentiality.

Fraudulent Use of a Database: ChoicePoint

- ChoicePoint is one of the largest sellers of private consumer data. In February, 2005 an identity theft ring used false documentation to open 50 accounts with ChoicePoint for a fee of $100-200 per account. This permitted them to gain access to personal data including social security numbers of thousands of consumers. ChoicePoint notified customers whose data had been disclosed only after being notified that state laws in California required consumer notification.

Privacy and Confidentiality: Data Mining

- A woman in Texas received a letter containing personal details about her and threatening her with rape. A convicted rapist who was serving time in a Texas prison had written the letter. He was entering data for a data mining company that had obtained the information from a product questionnaire that the woman had filled out and sent back to the company.

The Lotus-Equifax Household Products Controversy

- Lotus developed a product in cooperation with Equifax, one of the three major credit card bureau companies in the U.S.
- Equifax collected data on consumers from a variety of sources including a consumer's credit history acquired from banks, employment history and payment records from creditors.
- The new product, Lotus Marketplace, would enable small businesses and other organizations to purchase targeted mailing lists to be used in direct mail marketing campaigns.

Tracing Syphilis in Cyberspace

- A syphilis outbreak occurred among gay men who met sex partners through an Internet chat room. Privacy protections prevented public health officials from learning the identities of the sex partners. The Internet service provider that hosted the chat room refused to release identifying information without a federal subpoena.

Genetic Information in Centralized Databases

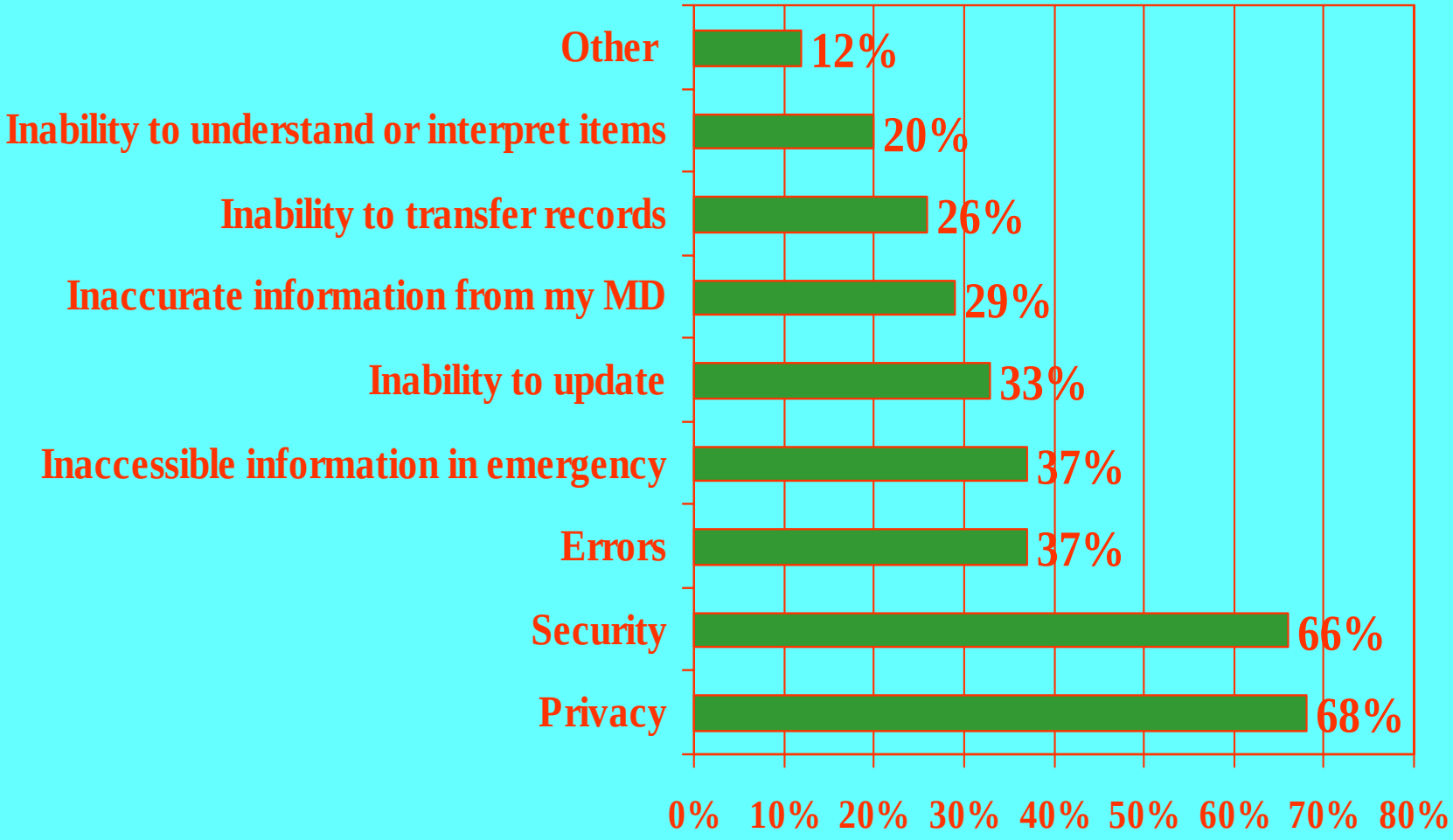
- Individual genetic information is increasingly stored in public, private, and government health databases.
- The data bases could be used for clinical practice, epidemiologic research, pharmaceutical investigations and other purposes

Reprinted with permission from Creators Syndicate.

Clinical Trials

- An ALS specialist suggested that a few of his patients try Neurontin, a drug that had been approved for epilepsy, and some of his patients shared this information online with other patients. Immediately other ALS patients began to demand access to the drug even though it had not been tested for ALS in clinical trials. As many as 30,000 ALS patients may have taken the drug. This created problems for investigators running clinical trials who feared that some patients enrolled in the clinical trials had also taken Neurontin.

Concerns about Keeping Online Health Records

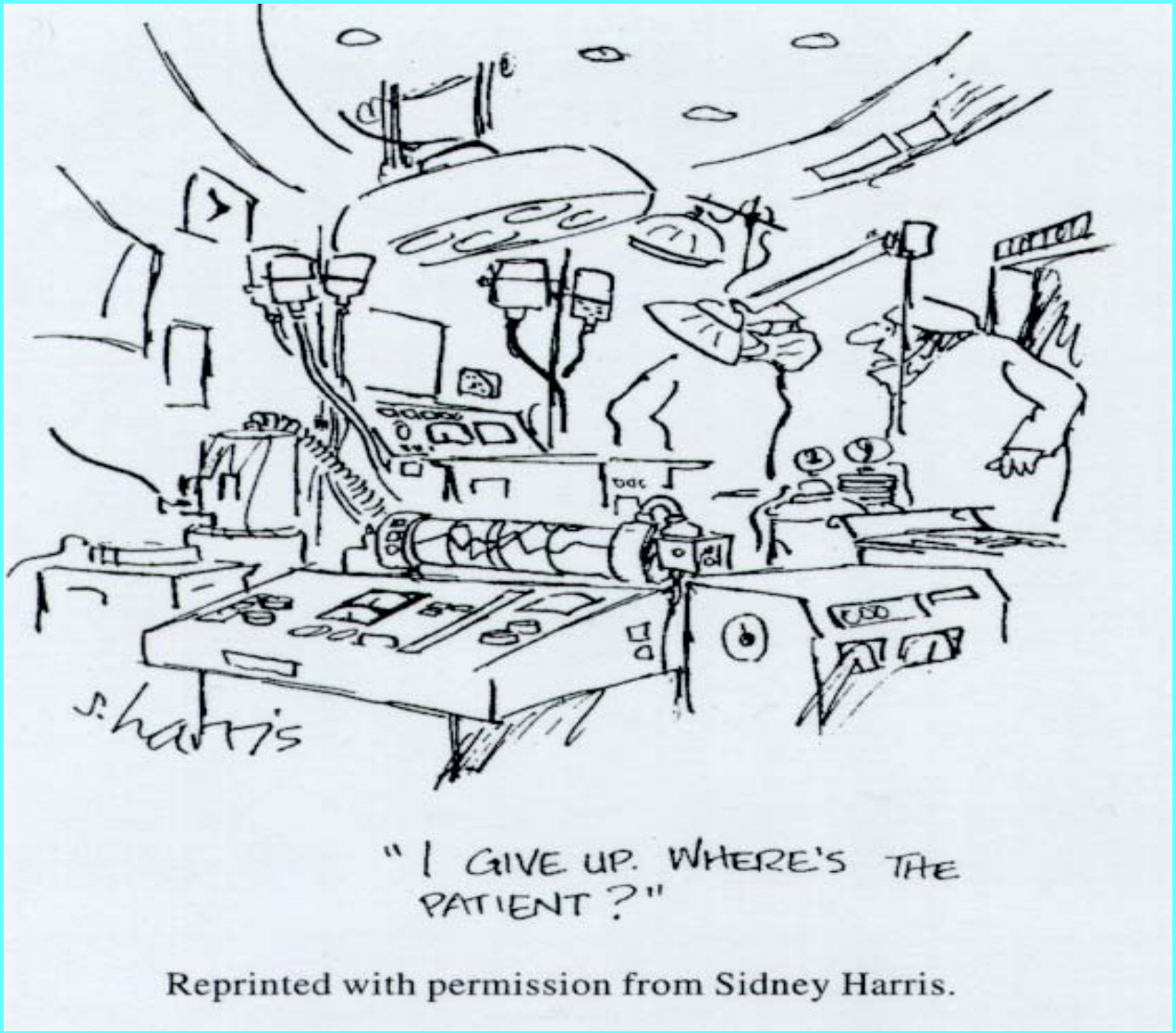


Cultural Change

- Health/Medical informatics has the potential to change the organizational structure and delivery of health services.
- Potential benefits include: more cost-effective health care, reduction of medical errors, better management of chronic disease, greater patient responsibility for the patient's own health care.

The Need for Public Policy

- EMR systems are critical to support integrated health care delivery systems
- EMRs are vulnerable to inappropriate use.
- A policy framework is needed to direct future development and private investment in IT.
- Absence of policies creates confusion about privacy rights
- Pending legislation contains conflicting proposals that will need to be resolved.



Reprinted with permission from Sidney Harris.

Case Insurance Companies

- Mr. D tried to increase his life insurance and was turned down by three insurance companies. He later learned that information that he had given to his physician in confidence had been included in thre MIB files that are used by insurance companies to determine eligibility of applicants.

ROLE OF CONFIDENTIALITY

- Respect Patient's Privacy.
- Establish Trust.
- Obtain Information Necessary for Treatment.
- Protect Patient form Potential Harm.

LIMITS TO CONFIDENTIALITY

- Modern High-Technology Health Care.
- Rights of the Community (Public Health).
- Threats to a Third Party.
- Allowing Patient to Harm Him/Herself.

Illustration by Dave Harbaugh

"He's not learning to play the harmonica . . . It's just confidential when he discusses the patient's medication on his cell phone."

Growth of Health Care Information Technology

- The health care industry spends $15 billion annually.
- The industry is expected to grow 20% annually.
- There are 35 publicly traded companies with market capitalization of $25 billion.

Public Concerns about Privacy

- 24% of health care providers reported violations of patients' privacy.
- 18% of the public felt that it was inappropriate to use patient data without consent.
- 75% of the public felt that it was inappropriate to use prescription data to detect fraud.
- 11% of the public reported not filing insurance claims to protect their privacy.

Case - Errors

- A certified sex therapist operated a Web site to treat people for sexual dysfunction. In March 1999, the sexual and medical histories of 15 women and 75 men who had consulted the doctor were inadvertently posted on a public Web site.

Case - Curiosity

- The medical team caring for a local celebrity became concerned about the level of interest in their patient's well-being. Staff members noted that a large number of hospital employees, some of whose names they didn't recognize, had accessed the patient's electronic medical record.

Public Policy Issues

- Existing laws only cover data collected by federal agencies.
- These laws do not cover secondary users of health information.
- There is a lack of incentives for institutions to invest in security of health information.

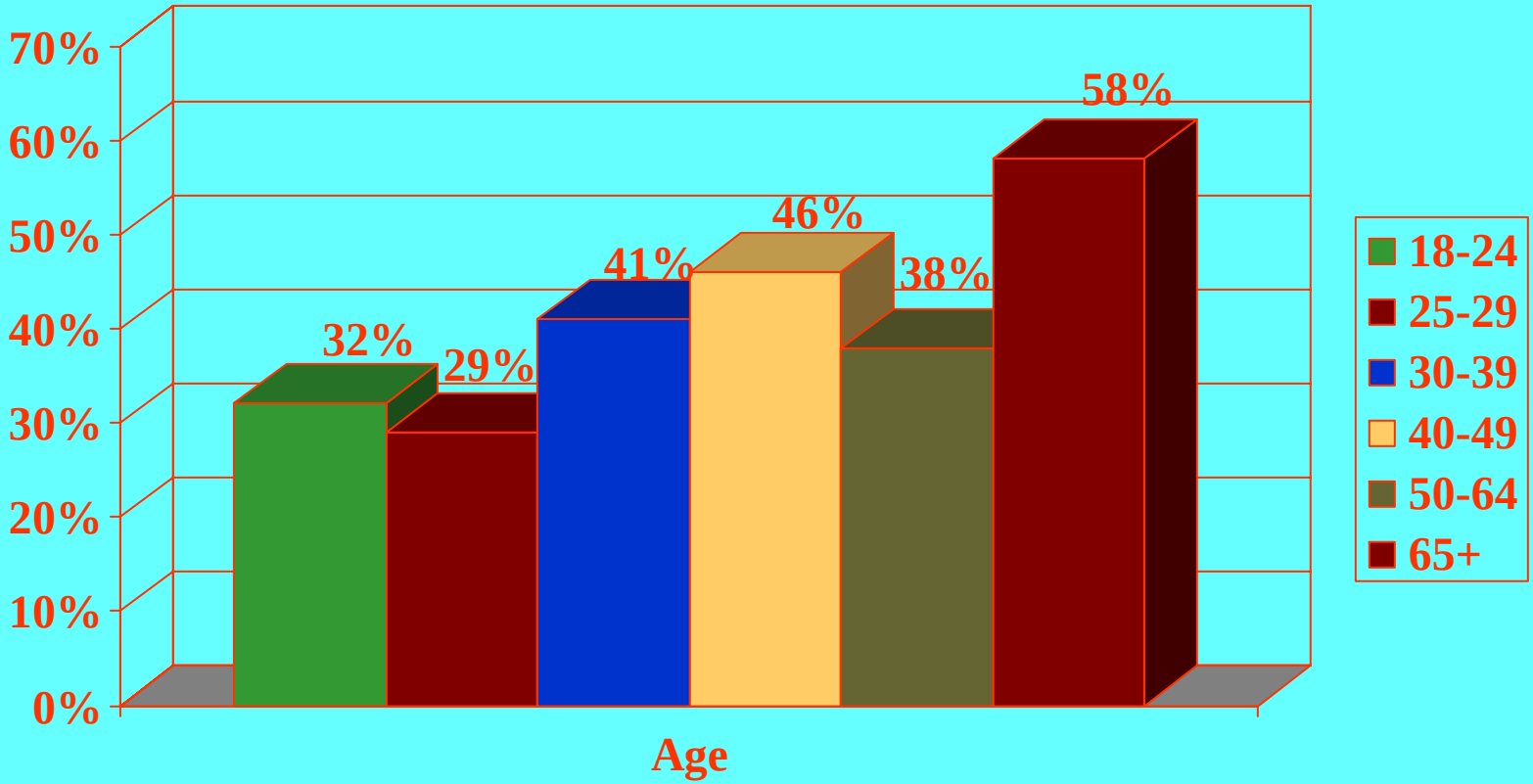
The Health Insurance Portability and Accountability Act of 1996.

- Only covers health information transmitted electronically.
- Does not cover insurance companies, pharmacies and direct marketers of personal data.
- Permits use of health information with patient identifiers for health care operations.

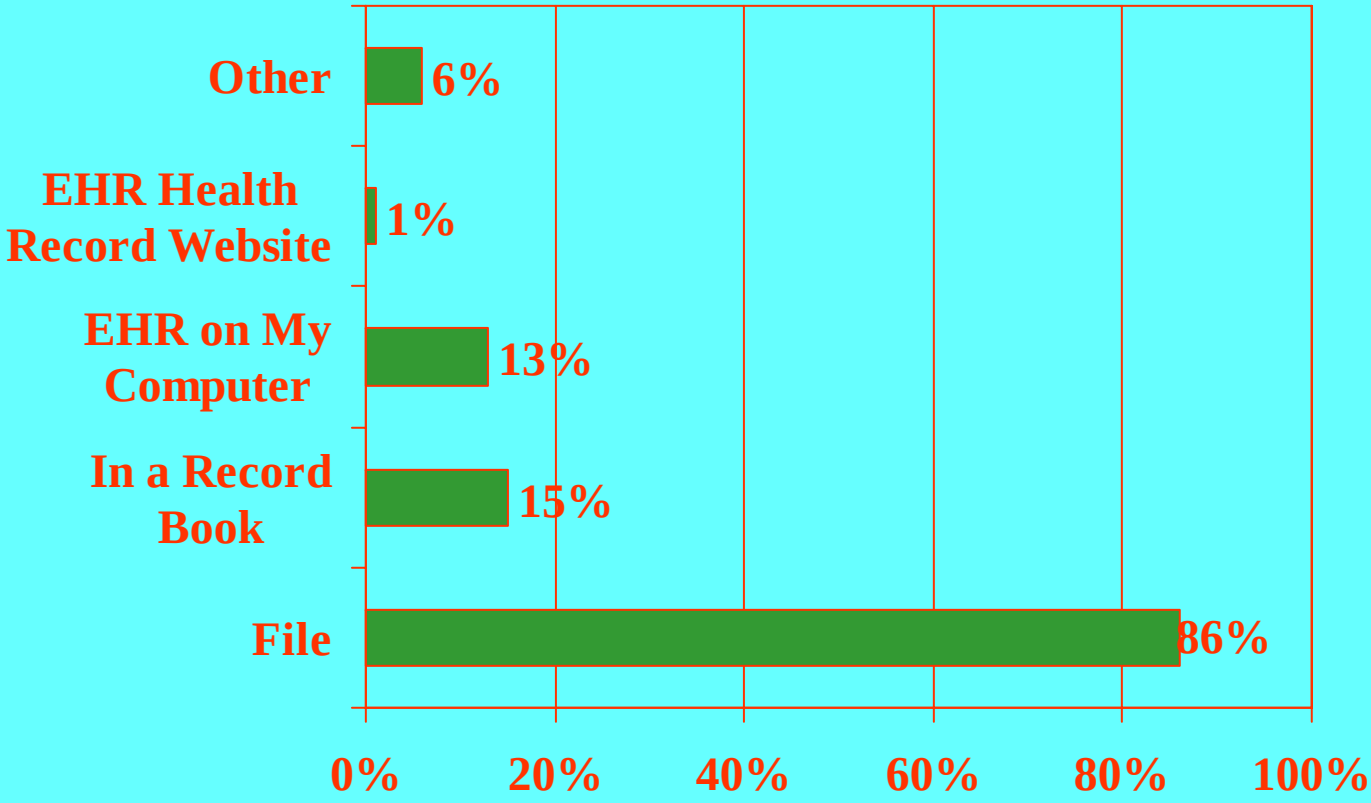
The Health Insurance Portability and Accountability Act of 1996.

- May allow sale of patient data for secondary use.
- Privately funded research is exempt form the regulations.
- There is concern over the use of a unique patient identifier.
- There are differences in regulations between the E.U. and the U.S.

Do You Have a Personal or Family Health Record?



In What Form do You Keep You Health Record?



Reasons for Keeping a Health Record