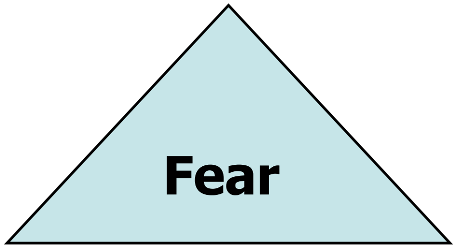
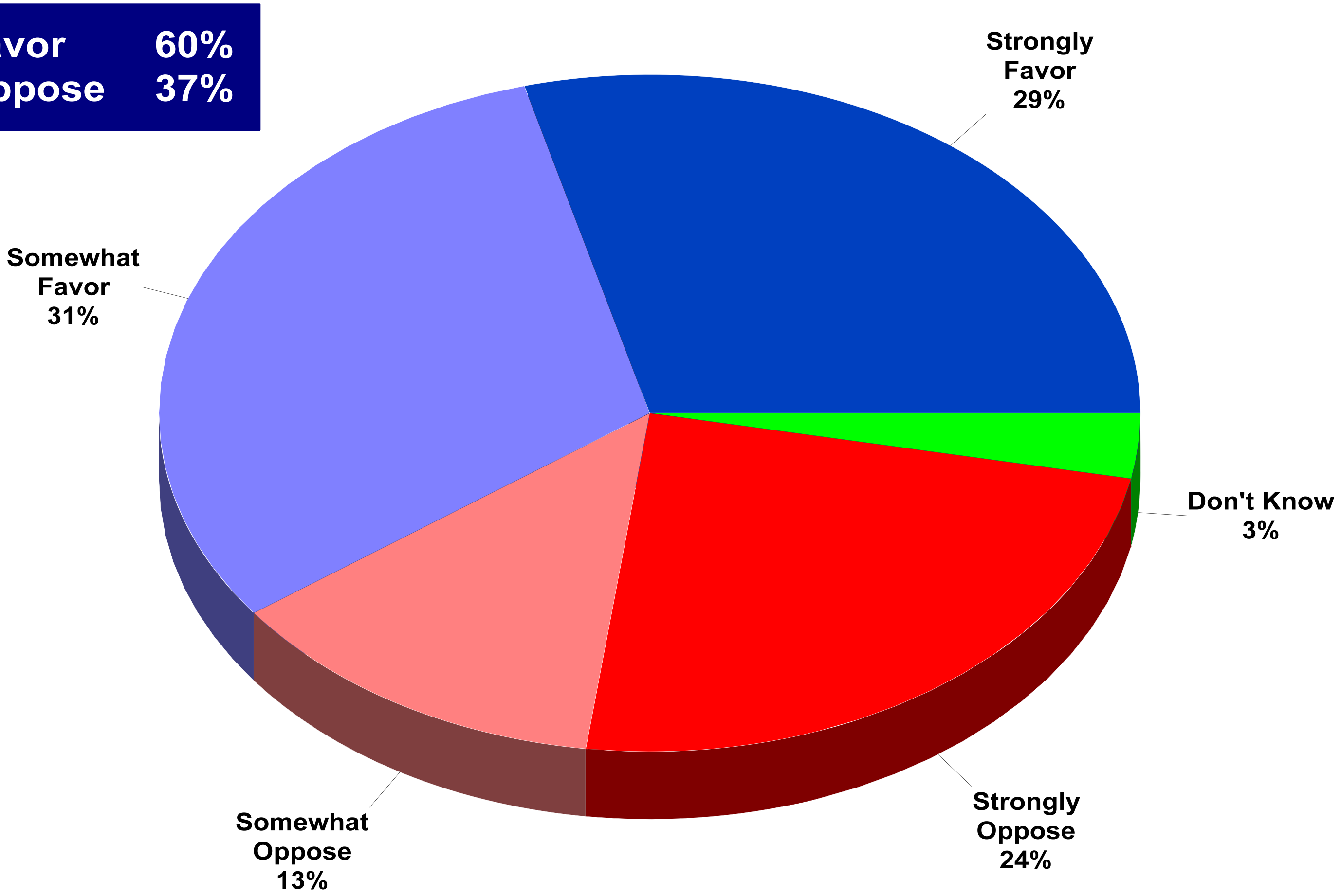


Fear

What do we know from public opinion surveys and focus groups?

Overall six out of ten Americans say they would favor the creation of a secure online “personal health record” service for their own use.

Total Favor	60%
Total Oppose	37%



Now, overall, would you favor or oppose the creation of this type of secure online "personal health record" service?

There is also a strong interest among consumers in using health information technology to more fully participate in their own health care.

Statement	% Yes
Check for mistakes in your medical record.	69%
Check and fill prescriptions.	68%
Get results over the Internet.	58%
Conduct secure and private email communication with your doctor or doctors.	57%

Now let's imagine that a new secure online service was made available to you allowing you to locate your medical records and view them through your own secure online "personal health record" account. Now I am going to read you some things this secure online "personal health record" service would allow you to do after I read each item, please tell me, yes or no, whether or not you would use this secure online "personal health record" service for each activity.

But…

California Health Care Foundation (2005)

- **67% of Americans are concerned about the privacy** of their personal medical records--recent privacy breaches have raised their level of concern
- **1 in 8 Americans have put their health at risk** by engaging in privacy-protective behavior:
  - *Avoiding their regular doctor*
  - *Asking a doctor to alter a diagnosis*
  - *Paying privately for a test*
  - *Avoiding tests altogether*

Harris/Westin poll on EHRs and Privacy (2006)

- **42% of Americans feel that "*privacy risks outweigh expected benefits*" from health IT.**

Keeping electronic medical information private and secure remains chief among consumer concerns.

Statement	% Absolute Top Priority
The identity of anyone using the system would be carefully confirmed to prevent any unauthorized access or any cases of mistaken identity.	91%
An individual would be able to review who has had access to their personal health information.	81%
Only with an individual's permission could their medical information be shared through this network.	79%
Employers would NOT have access to the secure health information exchange networks.	68%

I am going to read you different attributes that could be part of this exchange or network and I would like you to rate the importance of each. As you respond, please keep in mind that not every attribute can be a top priority.

Americans recognize the “upside”… and the “downside”…

- Fear of misuses
  - 52% believe employer uses medical info to affect personnel or insurance benefits (CHCF Survey 2005)
  - 85% believe if genetic test results known to insurers, would refuse policies or charge more (Genetics and Public Policy Center Survey 2007)
- Three-quarters of Americans are willing to share their personal information to help public officials look for disease outbreaks and research ways to improve the quality of health care if they have safeguards to protect their identity (Markle Survey 2006).

Markle Survey
November 2006

- ***3/4 want the government to set rules*** **to protect** the privacy and confidentiality of electronic health information

- ***2/3 want the government to set rules*** *controlling the secondary uses of information*

What is HIPAA?

Health Insurance Portability and Accountability Act

- Privacy Legislation (Finalized Dec 2000 - Compliance 4/14/03)
- Security Standards
- Electronic Data Interchange (EDI) Transaction and Code Sets (Finalized 8/17/00 - Compliance 10/16/02)

- The potential penalties for non-compliance apply to individuals and institution
  - Civil and criminal penalties
  - Fines up to $250,000
  - Imprisonment up to 10 years

WHAT IS HIPAA IN PRINCIPLE?

- The concept of HIPAA’s Privacy and Security Regulations is simple:

KEEP INDIVIDUALS’ HEALTH INFORMATION SECURELY CONFIDENTIAL

HIPAA is a major cultural change away from the notion of a healthcare provider’s “ownership” of an individual’s medical record.

HIPAA represents the
consumer-based concept
of an individual’s ownership of
her/his personal health
information,
which may be given in
custody to a health care
provider for defined, limited
specific purposes.

What does HIPAA mean operationally?

It’s all about Protected Health Information (PHI).

HIPAA requires

- **procedural,**
- **physical and**
- **electronic safeguards**

to protect the privacy and confidentiality of PHI

Often it is not just about IT !

Backup Slides

What is “Protected Health Information”?

PHI means any information, whether oral or recorded, in any form or medium, that:

a) Is created or received by a healthcare provider, health plan, public health authority, employer, the insurer, school or university or health clearinghouse; and

b) Relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

c) Permits identification of the individual or could reasonably be used to identify the individual.

What are some examples of HIPAA Privacy Operational Requirements for Health Care Providers?

- Post “Notice of Information Practices” and provide a copy to each patient
- Obtain written consent from each patient for treatment, payment, and healthcare operations
- Restrict access to PHI by in-house personnel to a “need to know” basis
- Maintain a record of all disclosures of the PHI
- Provide for individual patient access to copies of his/her PHI, and creating a process for requesting amendment of the PHI record and reviewing the record of disclosures.
- Use PHI only for treatment (including payment and healthcare operations) unless otherwise authorized.
- Comply with HIPAA regulations for disclosure of PHI for purposes other than the consented healthcare.
- Establish Business Associate agreements

What are some examples of HIPAA Privacy Operational Requirements for Using PHI for Research?

- Obtain each individual’s written authorization for disclosure of specified PHI for the specific research use

OR

- Obtain a waiver of the authorization requirement from our IRB and hope that the waiver will be accepted by the healthcare provider (or other covered entity)

OR

- Seek completely de-identified (per HIPAA Standards) information such that it is no longer truly PHI.

Security

- Security Standards
  - HCFA issued proposed standards August 12, 1998, but final rules have not been issued yet
  - Most healthcare organizations will be required to comply within two (2) years of final rule
  - Covers all healthcare entities that maintain or transmit electronic “health information”
  - Proposed standards address electronic information only

Security cont…

- The regulatory requirements must be addressed, but how that is done is up to the organization administratively and technically
- Risk Analysis is required by the regulations
- No compliance checklist

Security Standards
It’s not just about IT

Administrative Procedures	Technical Security Services
• Certification • Chain of Trust Partner Agreement • Contingency Plan • Formal Mechanism for record processing • Information access control • Internal Audit • Personnel Security • Security Configuration Management • Security Incident process • Security Management Process • Termination Procedures • Training	• Access Control • Audit Controls • Authorization Control • Data Authentication • Entity Authentication ⇒ Automatic Logoff ⇒ Unique User Identification ⇒ Password/PIN/Biometric/Token ⇒ Telephone Callback
• Assigned Security Responsibility • Media Controls • Physical access controls • Policy/guidelines on workstation use • Secure work station location • Security Awareness training	• Communications / network controls ⇒ Access Controls / Encryption / Audit Trails / Event reporting / Integrity Cntrls • Digital Signature (Optional)
Physical Safeguards	**Technical Security Mechanisms**

HIPAA Security Matrix

Security Impact

- Security management process
  - Documented risk assessment
  - Security & Sanction policies
    - User accountability for the protection of PHI maintained on any medium (server, pc, laptop, pda, etc…)
- Documented termination procedures
  - Timely removal of systems access, retrieval of keys, changing of system passwords, combination locks, etc…
- Virus protection

Security Impact

- Encryption of transmitted information via the internet (e-mail, web browsers)
- Access Controls
  - Unique user identification & authorization (NO Group Accounts!)
  - Access must be limited to the minimum required to perform business function
- Hardware/software controls – Policies and procedures that govern the receipt and removal of hardware and software into and out of a facility.
- Security training/awareness

Security Impact

- Physical access controls for systems containing PHI
  - Disaster recovery plan
  - Facility security plan
  - Visitor sign in and/or escorts
- Workstation controls
  - Physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to PHI
- Chain of Trust Partner Agreements
- Certification of all IT systems