Privacy, Confidentiality, and Security

Component 2/Unit 8c

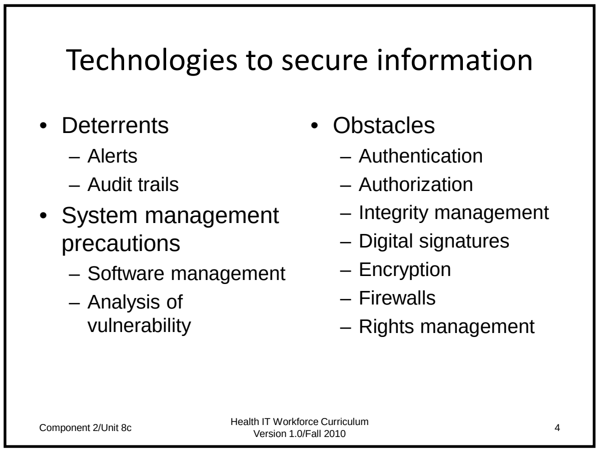
Tools for protecting health information

- IOM report: *For the Record* (1997)
- Report commissioned by NLM; informed HIPAA legistation
- Looked at current practices at six institutions
- Recommended immediate and future best practices
- Some content dated, but framework not

For the Record
Protecting Electronic Health Information
Infectious
Disease
Allergies
COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD
NATIONAL RESEARCH COUNCIL

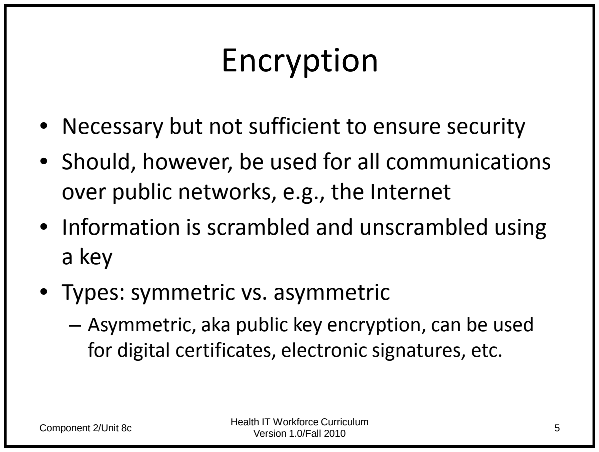
Threats to security

- Insider
  - – Accidental disclosure
  - – Curiosity
  - – Subornation
- Secondary use settings
- Outside institution
  - – A lot of press, few examples



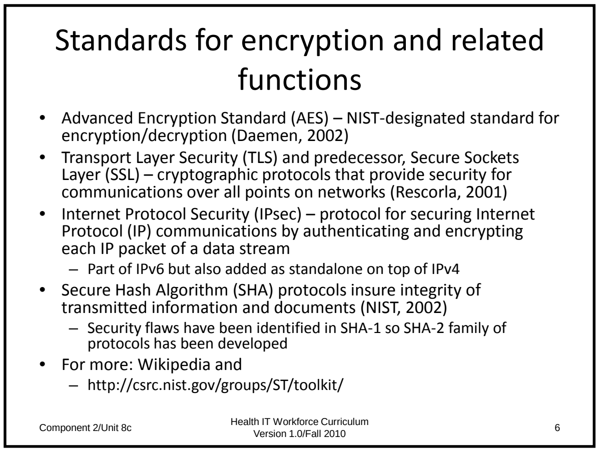
Technologies to secure information

- Deterrents
  - Alerts
  - Audit trails
- System management precautions
  - Software management
  - Analysis of vulnerability
- Obstacles
  - Authentication
  - Authorization
  - Integrity management
  - Digital signatures
  - Encryption
  - Firewalls
  - Rights management



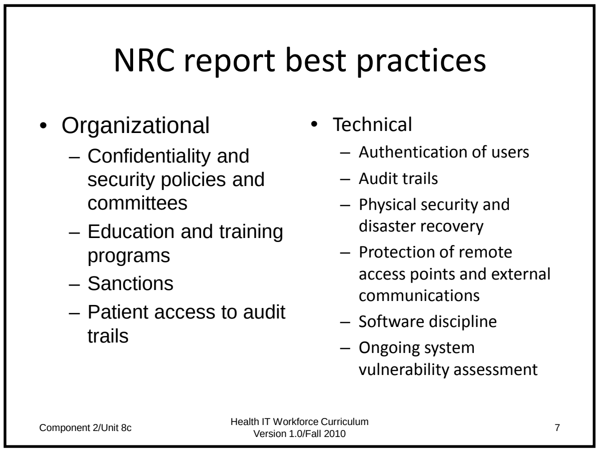
Encryption

- Necessary but not sufficient to ensure security
- Should, however, be used for all communications over public networks, e.g., the Internet
- Information is scrambled and unscrambled using a key
- Types: symmetric vs. asymmetric
  - Asymmetric, aka public key encryption, can be used for digital certificates, electronic signatures, etc.



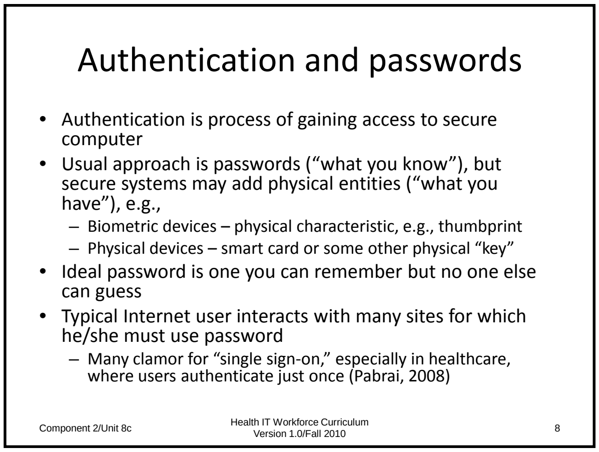
Standards for encryption and related functions

- Advanced Encryption Standard (AES) – NIST-designated standard for encryption/decryption (Daemen, 2002)
- Transport Layer Security (TLS) and predecessor, Secure Sockets Layer (SSL) – cryptographic protocols that provide security for communications over all points on networks (Rescorla, 2001)
- Internet Protocol Security (IPsec) – protocol for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream
  - Part of IPv6 but also added as standalone on top of IPv4
- Secure Hash Algorithm (SHA) protocols insure integrity of transmitted information and documents (NIST, 2002)
  - Security flaws have been identified in SHA-1 so SHA-2 family of protocols has been developed
- For more: Wikipedia and
  - http://csrc.nist.gov/groups/ST/toolkit/



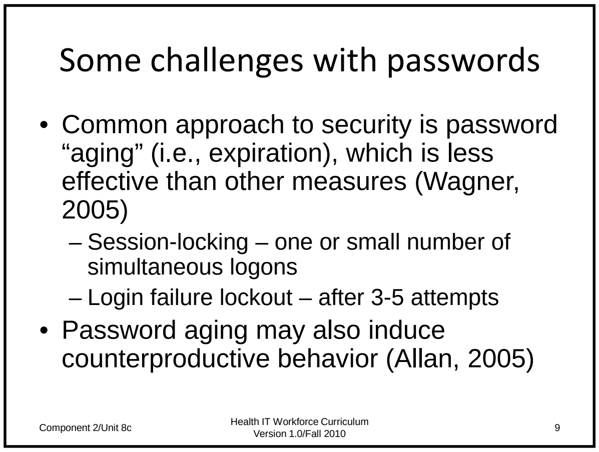
NRC report best practices

- Organizational
  - Confidentiality and security policies and committees
  - Education and training programs
  - Sanctions
  - Patient access to audit trails
- Technical
  - Authentication of users
  - Audit trails
  - Physical security and disaster recovery
  - Protection of remote access points and external communications
  - Software discipline
  - Ongoing system vulnerability assessment



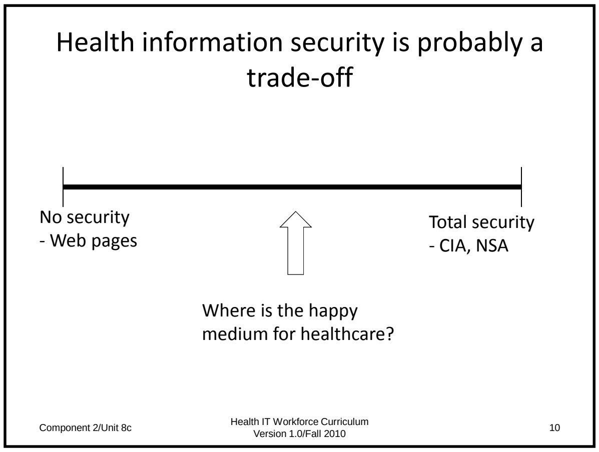
Authentication and passwords

- Authentication is process of gaining access to secure computer
- Usual approach is passwords ("what you know"), but secure systems may add physical entities ("what you have"), e.g.,
  - Biometric devices – physical characteristic, e.g., thumbprint
  - Physical devices – smart card or some other physical "key"
- Ideal password is one you can remember but no one else can guess
- Typical Internet user interacts with many sites for which he/she must use password
  - Many clamor for "single sign-on," especially in healthcare, where users authenticate just once (Pabrai, 2008)



Some challenges with passwords

- Common approach to security is password "aging" (i.e., expiration), which is less effective than other measures (Wagner, 2005)
  - Session-locking – one or small number of simultaneous logons
  - Login failure lockout – after 3-5 attempts
- Password aging may also induce counterproductive behavior (Allan, 2005)

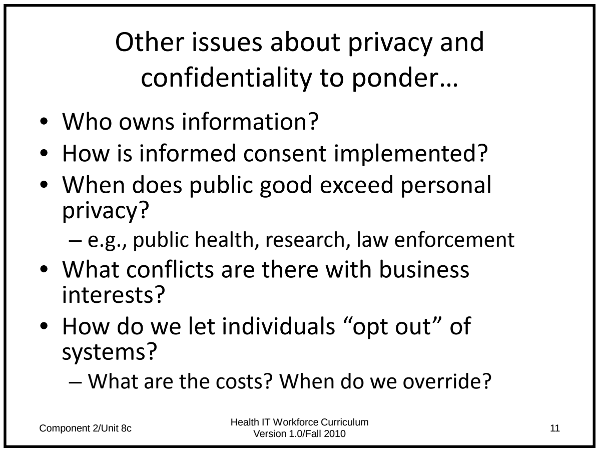


Health information security is probably a trade-off

No security
- Web pages

Total security
- CIA, NSA

Where is the happy medium for healthcare?



Other issues about privacy and confidentiality to ponder…

- Who owns information?
- How is informed consent implemented?
- When does public good exceed personal privacy?
  - e.g., public health, research, law enforcement
- What conflicts are there with business interests?
- How do we let individuals "opt out" of systems?
  - What are the costs? When do we override?