

7.4b Privacy and Security

10x10 – Introduction to Biomedical Informatics & Artificial Intelligence
William Hersh, MD, FACMI, FAMIA, FIAHSI
Copyright 2026, All Rights Reserved



Concerns about security

Data uses and potential points of leakage

A problem for paper too

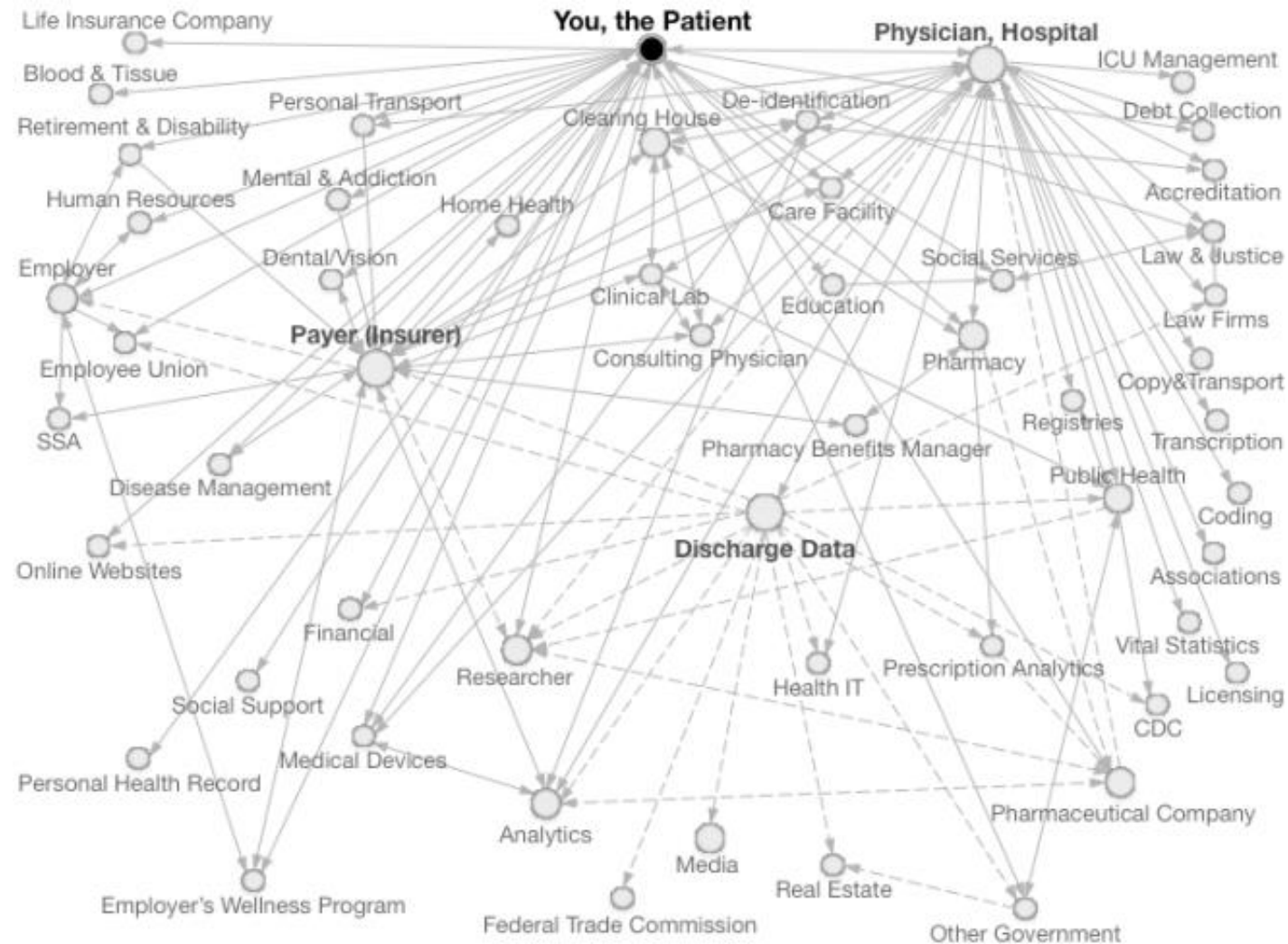
Consequences of poor security

Tools to protect security

7.4b - Hersh - AMIA



Another view of where data may go



Cannot forget that paper records have insecurity as well

Difficult to audit trail of paper chart

Fax machines are still used and easily accessible to people in offices

Records frequently copied for many reasons

- New providers, insurance purposes

Records abstracted for variety of purposes

- Research
- Quality assurance
- Insurance fraud – Medical Information Bureau (Rothfeder, 1992)

Potential consequences of poor security

Privacy-protective behaviors

- 13% of consumers admit to engaging in “privacy-protective” behaviors that might put health at risk (CHCF, 2005), such as
 - Asking doctor to lie about diagnosis
 - Paying for a test because they did not want to submit a claim
 - Avoid seeing their regular doctor
- Agaku (2014) – two-thirds of US adults have concern about breach when health data transmitted electronically; 12.3% have withheld information due to security concerns

Breach remediation efforts in hospitals associated with deterioration in timeliness of care and patient outcomes over 3 years (Choi, 2019)

- Time-to-electrocardiogram increased by 2.7 minutes
- 30-day acute MI mortality increased 0.36% in era of declining rates in general

Can undermine patient safety (Warner, 2022)

Tools for protecting health information

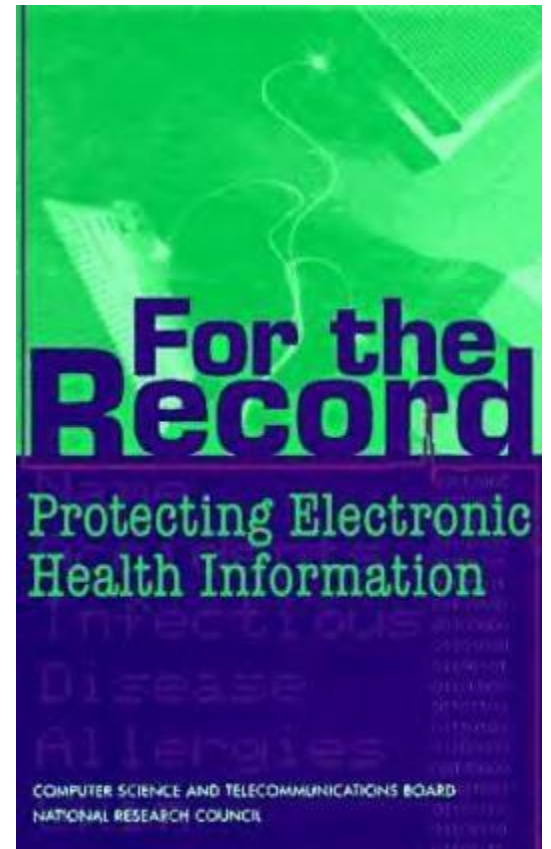
IOM report: For the Record (1997)

Report commissioned by NLM; informed HIPAA legislation

Looked at current practices at six institutions

Recommended immediate and future best practices

Most content dated, but framework not



Threats to security

Insider

- Accidental disclosure
- Curiosity
- Subornation

Secondary use settings

Outside institution

- A lot of press, few examples (back then, plenty more now)

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 be used for all devices, especially 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 information security

National Institute for Standards and Technology (NIST)

- [Computer Security Resource Center](#)

[ISO 27000 series](#) specifies best practices for telecommunications security

Medical device cybersecurity playbook (Chase, 2022)

Standards for Internet security include [OAuth2](#) for authentication and OpenID for identification

- Used by Google, Facebook, etc. to authenticate individuals
- Increasing use in healthcare, including in SMART on FHIR (Mandel, 2016)

[Best practices for secure APIs in healthcare](#)

Authentication and passwords

Authentication is process of gaining access to secure computer

- Most commonly done with user passwords

Typical user interacts with many professional and personal applications for which he/she must use password

- Many desire “single sign-on,” especially in healthcare, where users authenticate just once

Growing use of two/multi-factor authentication, i.e., in addition to passwords (“what you know”), may add physical entities (“what you have”), e.g., smart card, smartphone, or some other physical “key”

- Common example is Duo app used by many, including OHSU

Some challenges with passwords

Many practices based on outdated principles (Cheswick, 2012; Florêncio, 2014; Abbott, 2018)

Best password is one that user can remember but no one else can guess

- But systems and sites use different rules for length and make-up of passwords (Florenco, 2007)
- Users require so many that they re-use them, such that discovery of one can lead to access to many systems (Herley, 2009)
- Key-logging software (sometimes running without user knowing) can identify passwords (Herley, 2009)
- Poor password policies take user time and reduce usability of systems (Norman, 2009)

One common approach to security is password “aging” (i.e., expiration), which requires users to change their passwords periodically (Florêncio, 2014)

More challenges with passwords

We're sorry, but the password you have chosen does not meet the Library of Congress password policy requirements. Please review the following and try again.

Password requirements:

1. A password must contain at least sixteen (16) characters, including at least three (3) of the following types of characters:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters(~!@#\$%^&*_-+=`\|(){}[]:;'"<>,.?/)

2. A password cannot contain three of the same characters. For example, it cannot contain the word "eerie" because the letter "e" is used three times in this word.

3. A password cannot be changed more than once per day (24 hours)

4. You must change your password every sixty (60) days or when prompted by the system.

5. When you change your password, you cannot use any of the eleven (11) most recently used passwords for your eCO user account.



Recent changes in thinking on passwords

Highly influential early document was NIST 800-63, which advocated use of upper case letters, numbers, and special characters, changed regularly (Burr, 2004)

- Now, NIST says, “N3v\$r M1^d” (McMillan, 2017)

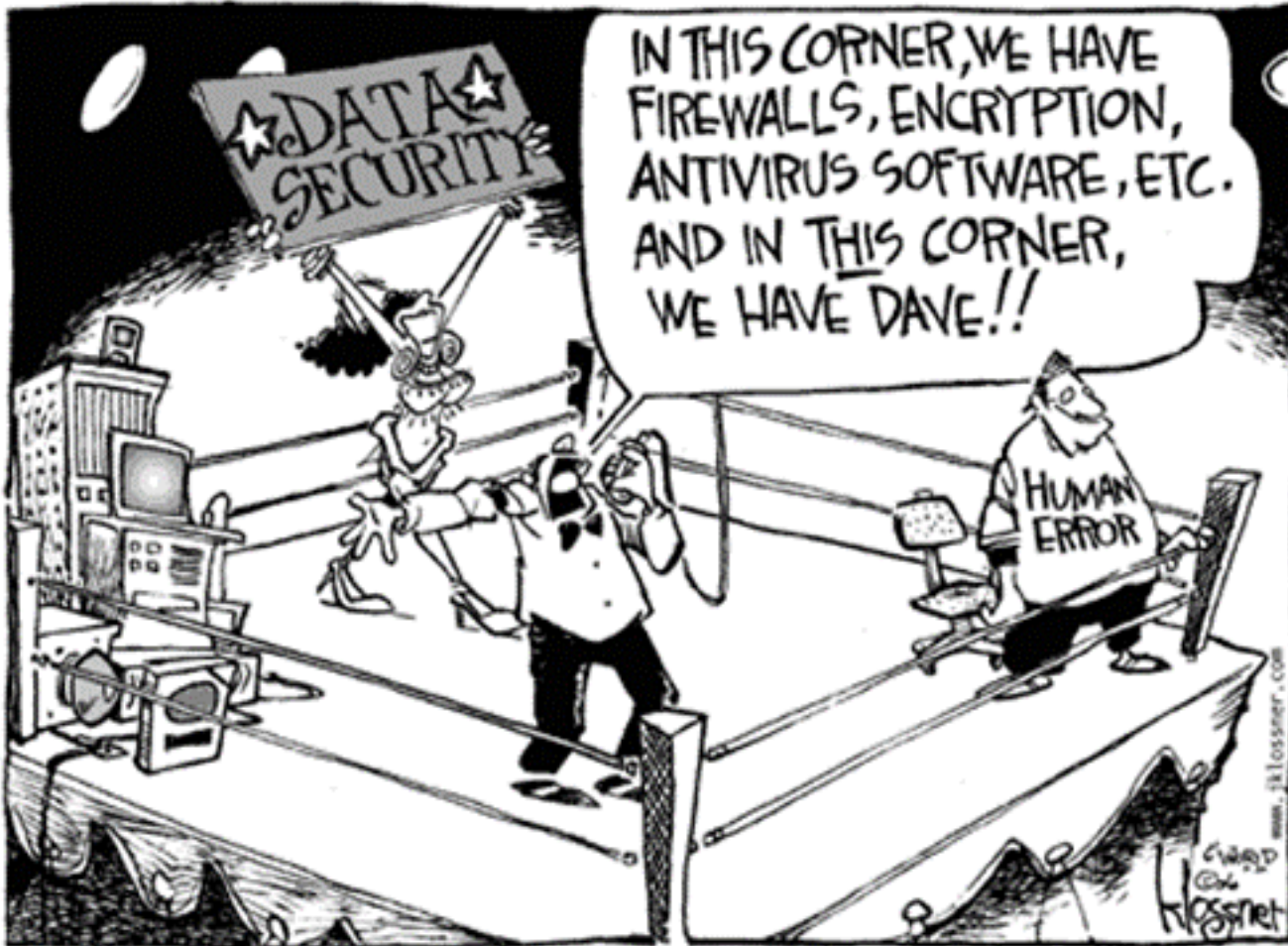
New recommendations (Grassi, 2020; Tan, 2020), summarized by Poza (2020)

- Length more important than complexity
- Eliminate periodic resets
- Show password while typing
- Allow pasting of password
- Use breached password protection
- Do not use password hints
- Limit password attempts
- Use multi-factor authentication

Or eliminate entirely? Growing advocacy for and use of passkeys, with authentication using smartphones and methods to unlock them (Amadeo, 2022)?

- Many industry partners supporting use through [FIDO Alliance](#)

Security challenges often come from users



"It's this new app—you put in your Social Security number, and it makes you look like a cat."

Security challenges often come from users (cont.)

“Good users do bad things” (Blythe, 2013)

Especially when rewarded by immediate gratification (Acquisti, 2004)

Patients and everyone else in healthcare system need good “data hygiene” (Blumenthal, 2015)

Many healthcare personnel admit to sharing passwords (Hassidim, 2017)

Half of documented HIPAA breaches due to user mistakes (Jiang, 2018)

Most malware and ransomware introduced by users (Nifakos, 2021)

Continued need for research on “cyber-hard” problems to add resilience to information systems (NAS, 2025)

Will blockchain solve our problems?

Distributed, linear, encrypted ledger (Kuo, 2017)

- Keeps immutable record of transactions, with details hidden by encryption

Basis for cryptocurrency (Nakamoto, 2008)

Impact beyond cryptocurrency modest, and many skeptical of larger use (Stinchcombe, 2018)

Also has substantial energy requirements (Huang, 2021) and exposes humans to significant pollution if powered by fossil fuels (Guidi, 2025)

What is role for blockchain in healthcare?

Use cases in healthcare (Halamka, 2018)

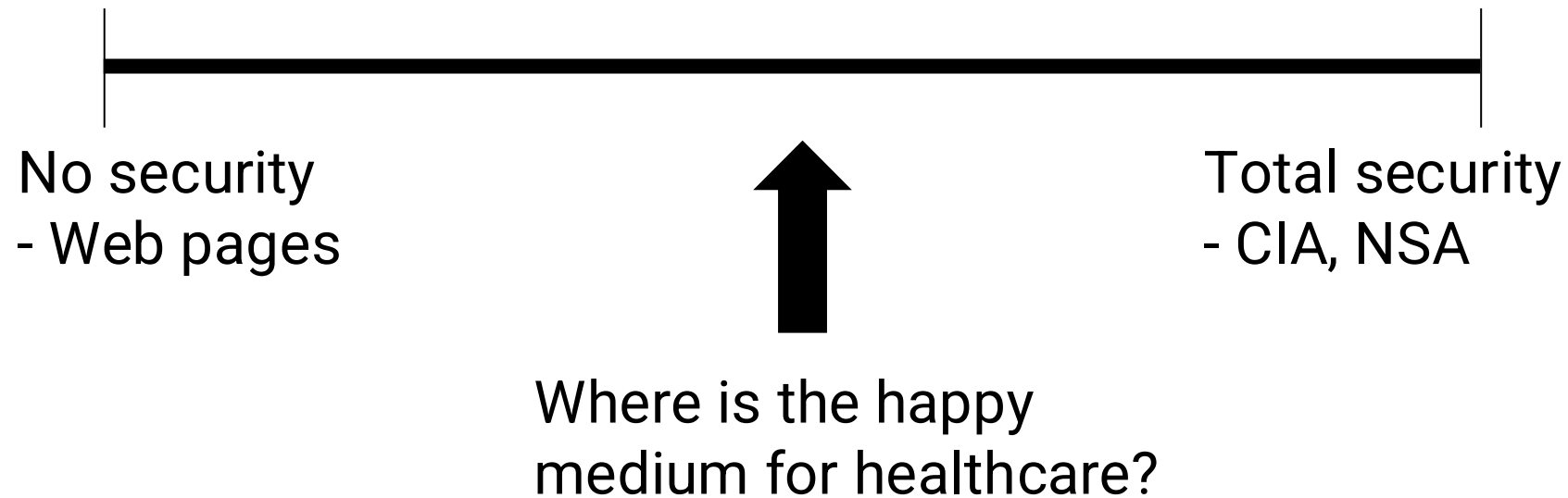
- Provide proof of work
- Guarantee data integrity
- Support economic model

Although does not solve other informatics challenges, such as standards and interoperability or general data security

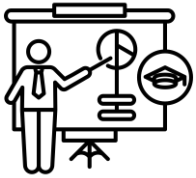
Role for guaranteeing integrity of data extracted from secure systems?

Use in healthcare minimal – use cases include decentralized internet of things (IoT) data storage, clinical trial management, biomedical certificate storage, EHR data sharing, and distributed predictive model generation but little operational use (Lacson, 2024)

Health information security is probably a trade-off



OHSU approach to cybersecurity (courtesy of Bridget Barnes, CIO)



TRAINING & AWARENESS

- Facilitate annual information privacy and security training, enabling workforce members to identify malicious emails, links, and files.
- Perform monthly phishing exercises.



EMAIL SECURITY ENHANCEMENTS

- All email originating outside OHSU is tagged with "EXTERNAL".
- Disallow the delivery of certain document types of attachments.
- Threat-aware email security filter.



REMOTE ACCESS ENHANCEMENTS

- Block third-party (non-OHSU) virtual private network connections.
- Require use of multifactor authentication (Duo)
- Review logs from multiple systems to detect anomalies.



ENDPOINT MANAGEMENT

- Maintain up-to-date endpoint detection and response systems to detect and isolate compromised devices.
- Maintain a robust endpoint patching program.
- Endpoint certificate management.



WEB FILTERING CONTROLS

- Maintain security systems to dynamically block malicious websites.
- Maintain similar controls for managed devices used off-network.



VULNERABILITY TESTING

- Scan all managed workstations, servers, and applications for vulnerabilities.
- Prioritize detected vulnerabilities and promptly patch to reduce risk.

Cybersecurity best practices

[ONC/ASTP Guide to Privacy & Security of Electronic Health Information](#)

[HHS 405d Aligning Health Care Industry Security Approaches](#)

[HHS HPH Cybersecurity Performance Goals](#)

[Healthcare and Public Health Cybersecurity](#)

[Health 3rd Party Trust \(Health3PT\) Initiative](#)

Many issues to ponder ...

Who owns information?

How is informed consent implemented?

When does public good exceed personal privacy?

- e.g., public health, research, law enforcement

How do we bring HIPAA into modern times?

What conflicts are there with business interests?

How do we let individuals “opt out” of systems?

- What are the costs and harms? When do we override?