COMPUTER SECURITY: Health Care Systems, Democracies and Social Networks

Roy Campbell

Week 2: **Health care systems** and their computer security concerns.

Friday Feb 10 9:30-11:00am.

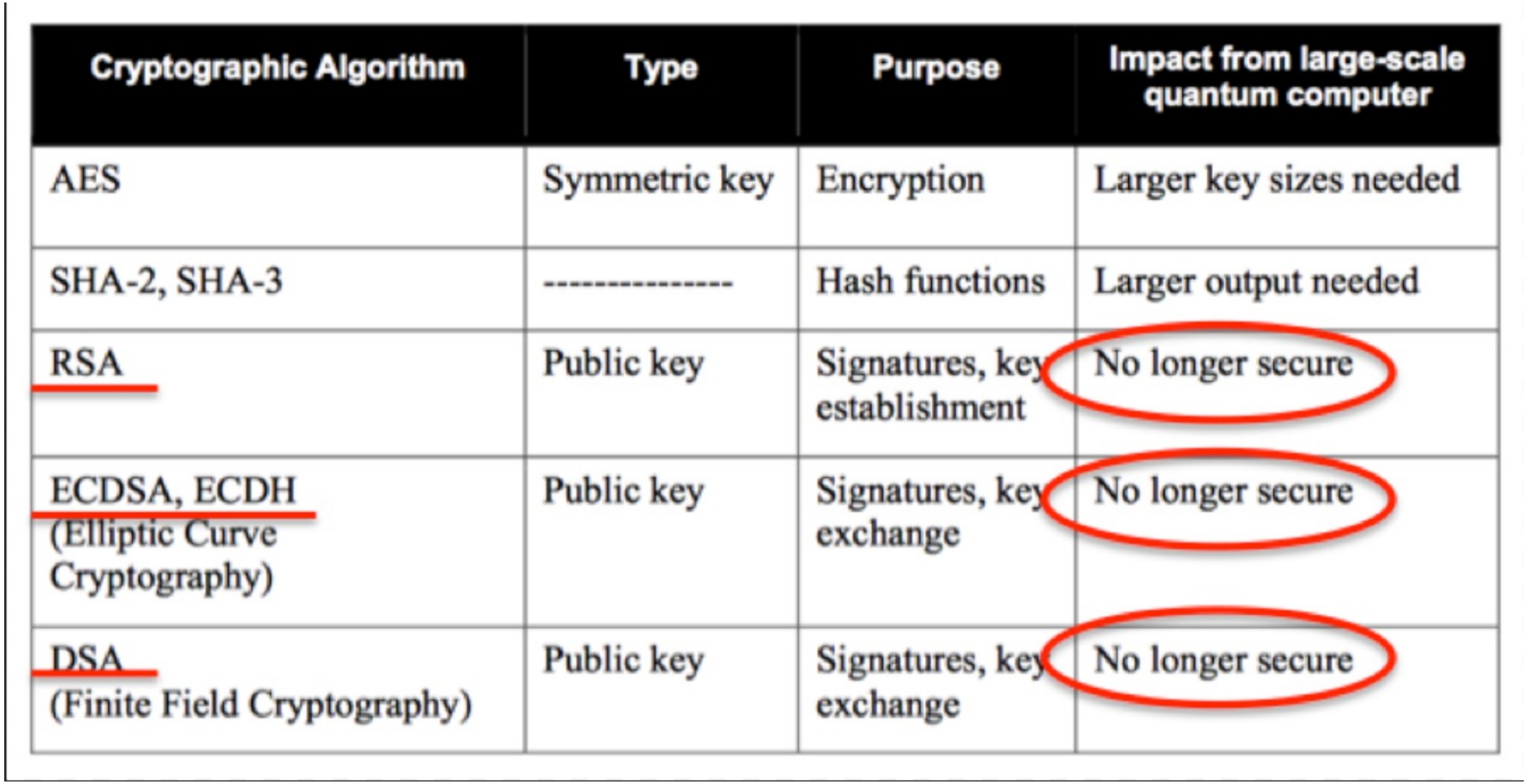
Osher Lifelong Learning Institute

Illinois Classroom

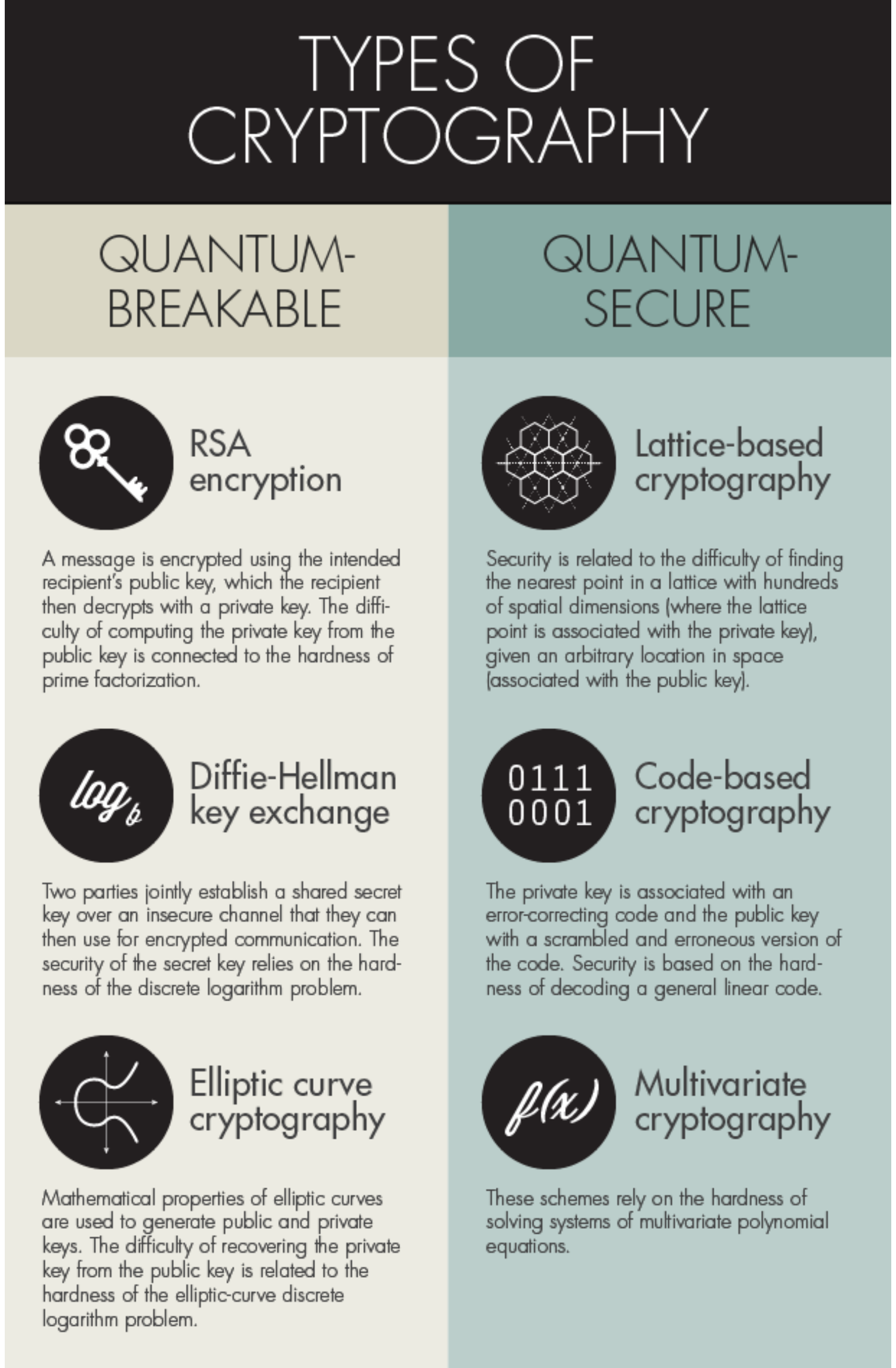
QUESTION FROM WEEK 1

- ***Bill Breeding: "This maybe outside the scope of this session but have read articles that say quantum computers will be able to undo the encryption most computers use today. Is this true or a realistic threat?"***
- Most encryption schemes can be broken given enough time to do it (measured in millennia.)
- The answer is yes, quantum computers could soon (20 years) be able to break the encryption schemes that are in use today quickly, especially those when used with a small 6-7 letter encryption key.
- However, they are not yet powerful enough (number of quantum bits) to do so.
- However, the science of encryption is developing schemes that will be proof against quantum computing.
- NIST Announced its approval of the first four Quantum-Resistant Cryptographic Algorithms (July 05, 2022): CRYSTALS-Kyber encryption algorithm and CRYSTALS-Dilithium, FALCON and SPHINCS for digital signatures. Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions.
- A new encryption draft standard for quantum proof encryption is to be announced in 2024 timeframe

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms



Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure


log_b
0111
0001
f(x)

TYPES OF CRYPTOGRAPHY

QUANTUM-BREAKABLE

RSA encryption

A message is encrypted using the intended recipient's public key, which the recipient then decrypts with a private key. The difficulty of computing the private key from the public key is connected to the hardness of prime factorization.

Diffie-Hellman key exchange

Two parties jointly establish a shared secret key over an insecure channel that they can then use for encrypted communication. The security of the secret key relies on the hardness of the discrete logarithm problem.

Elliptic curve cryptography

Mathematical properties of elliptic curves are used to generate public and private keys. The difficulty of recovering the private key from the public key is related to the hardness of the elliptic-curve discrete logarithm problem.

QUANTUM-SECURE

Lattice-based cryptography

Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where the lattice point is associated with the private key), given an arbitrary location in space (associated with the public key).

Code-based cryptography

The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code. Security is based on the hardness of decoding a general linear code.

Multivariate cryptography

These schemes rely on the hardness of solving systems of multivariate polynomial equations.

WEEK 2: COMPUTER SECURITY: HEALTH CARE SYSTEMS

1. Health care systems and their computer security concerns [5]
2. Major health care systems [14]

HOSPITAL GIVES STRAY CAT NEW JOB AS A SECURITY GUARD

#EMERGENCY-SERVICES.NEWS

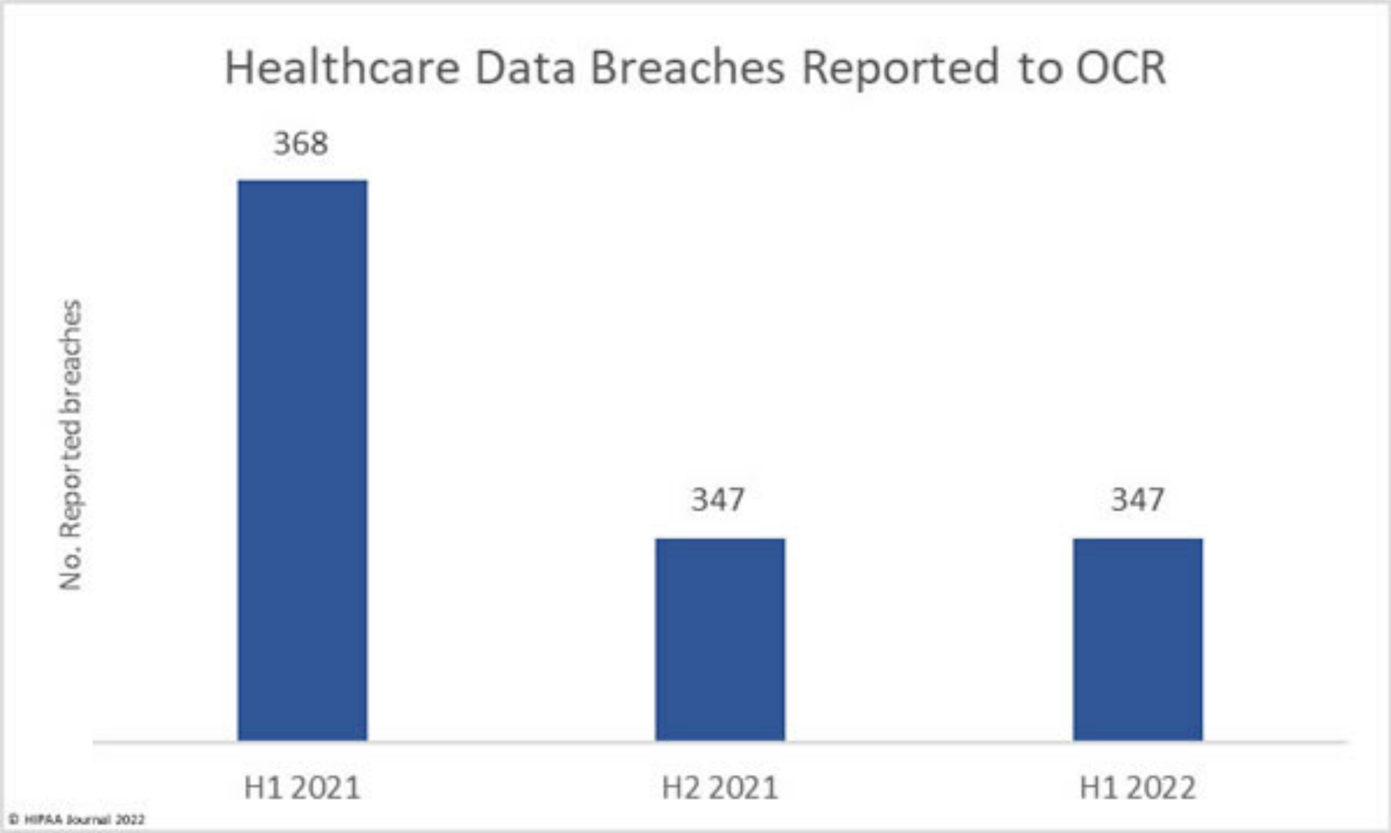
WEEK 2: COMPUTER SECURITY: HEALTH CARE SYSTEMS

1. **Health care systems and their computer security concerns**
2. Major health care systems
3. Health care insurance systems
4. HIPAA, privacy, clinical outcomes, financial resources
5. Recent attacks on health care systems, current controversies, and problems.
6. Practical safeguards

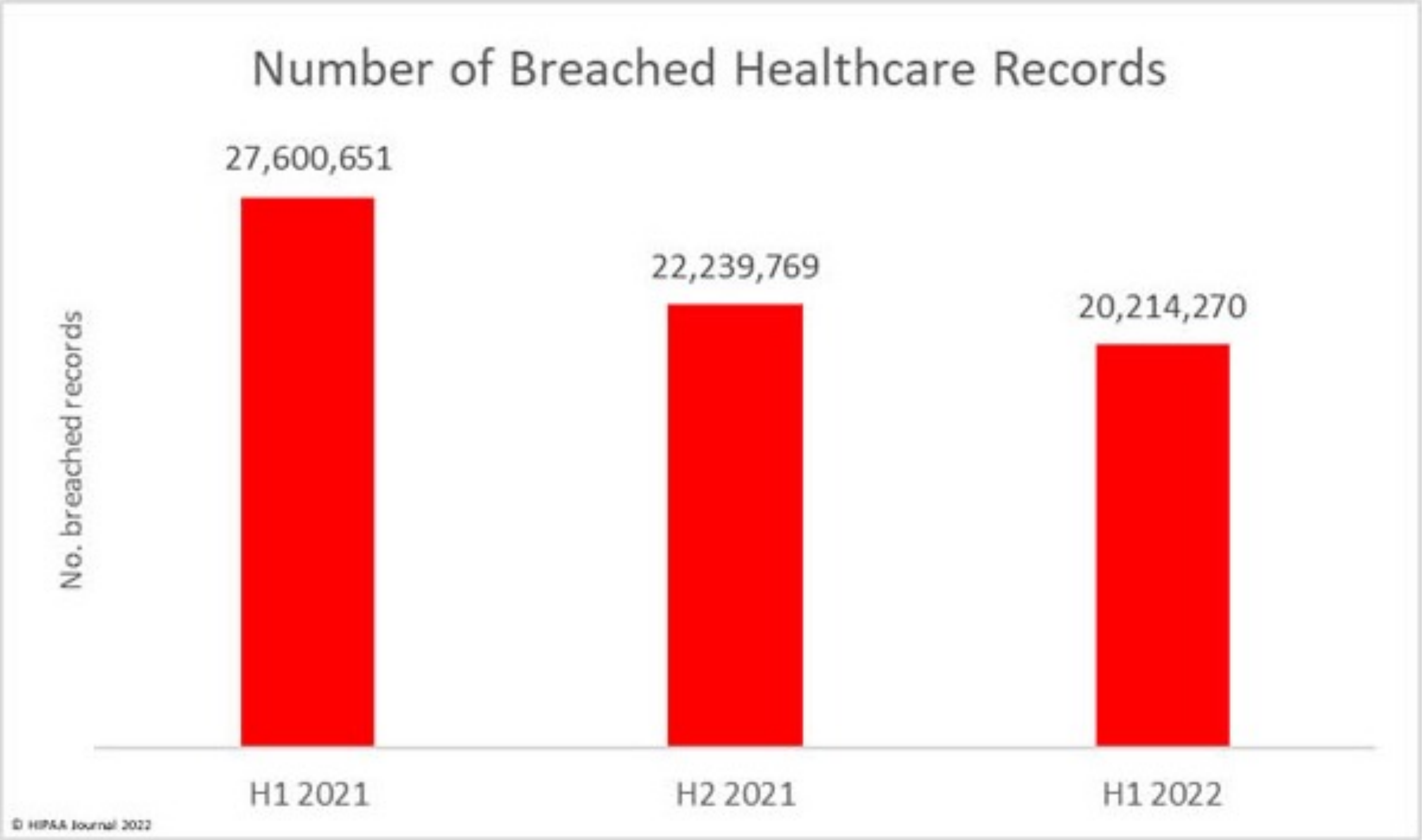
ATTACKS ON HEALTHCARE

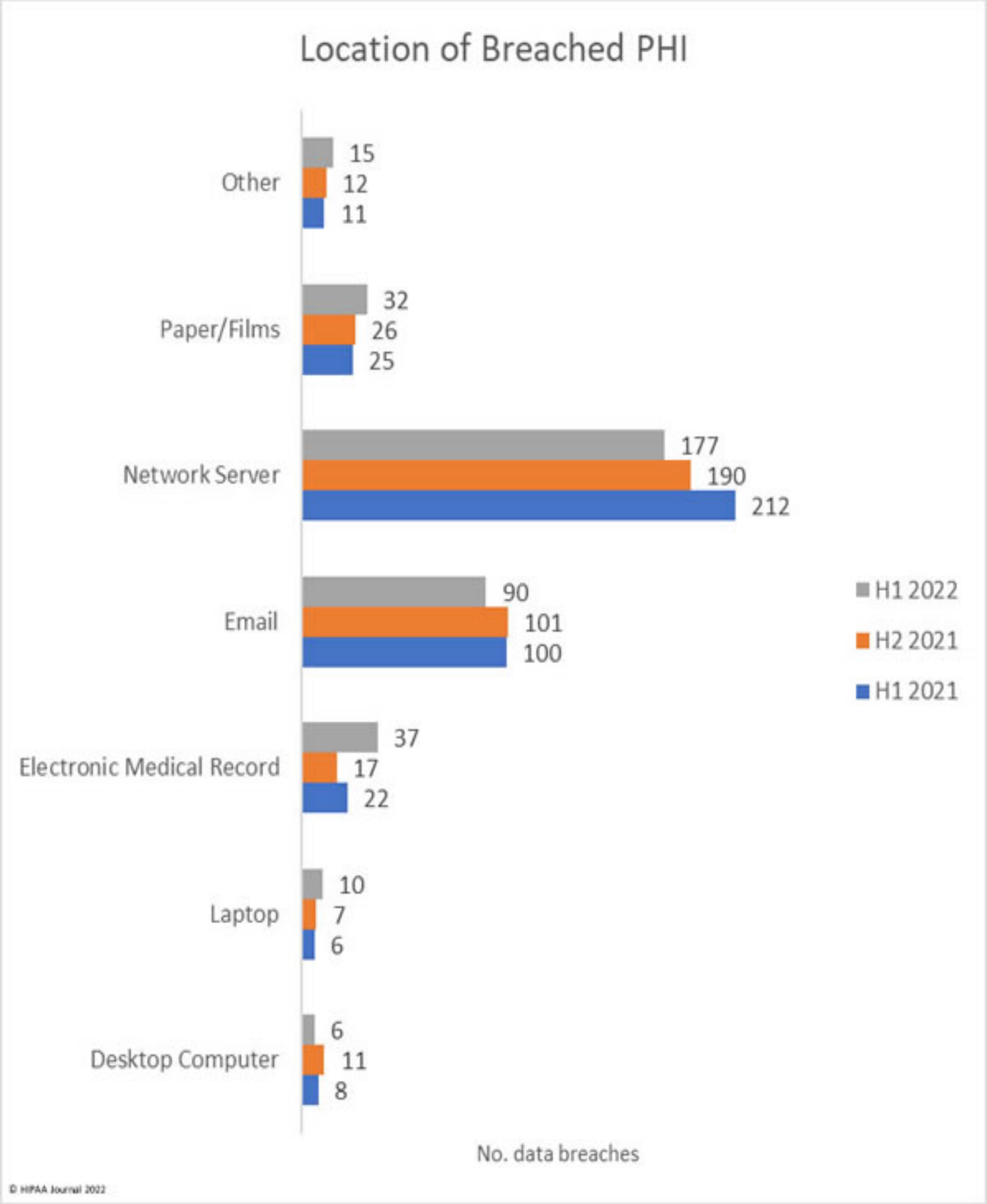
HTTPS://WWW.HIPAAJOURNAL.COM/1H-2022-HEALTHCARE-DATA-BREACH-REPORT/

- 347 healthcare data breaches of 500 or more records were reported to the Department of Health and Human Services' Office for Civil Rights" in the first half of 2022 alone.



NUMBER OF BREACHED HEALTHCARE RECORDS

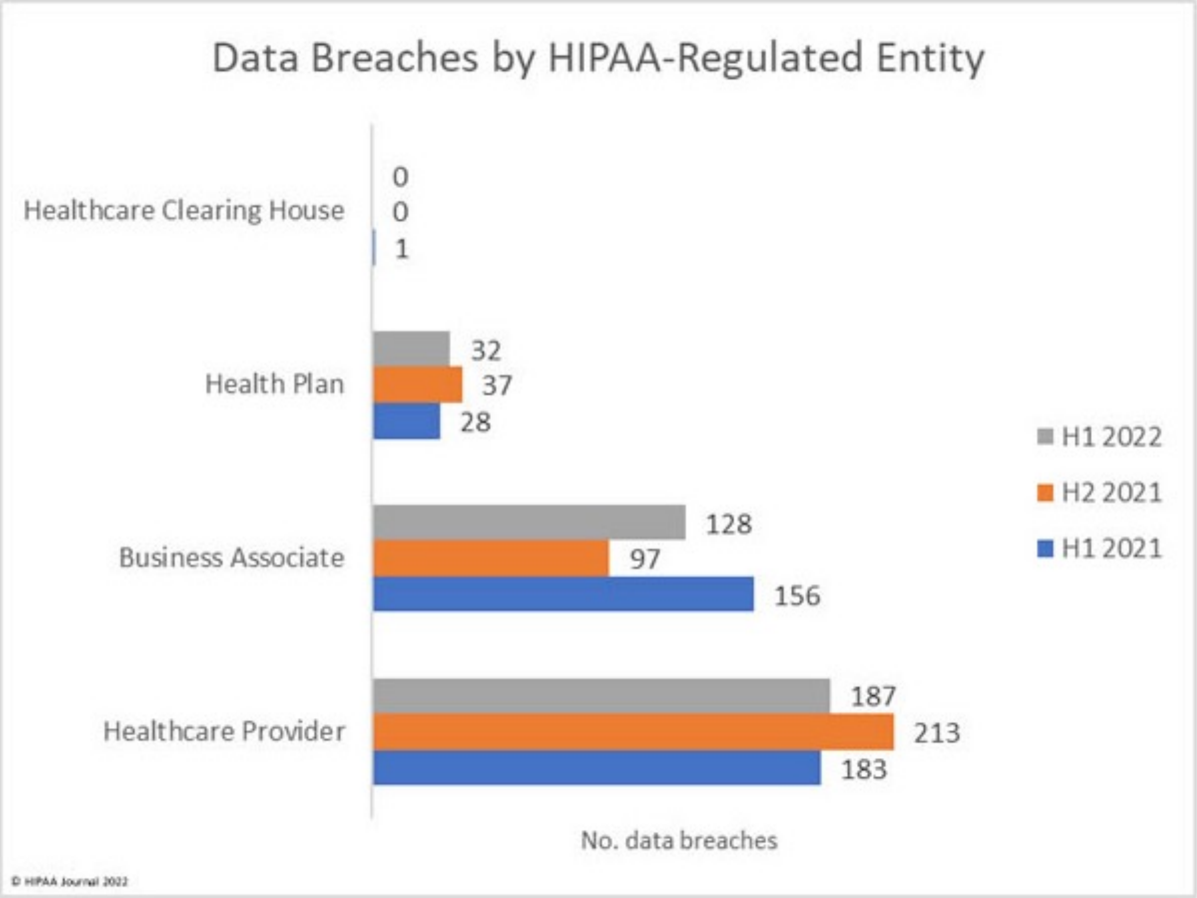




LOCATION OF BREACHES

Illinois reported 12 major breaches 2022

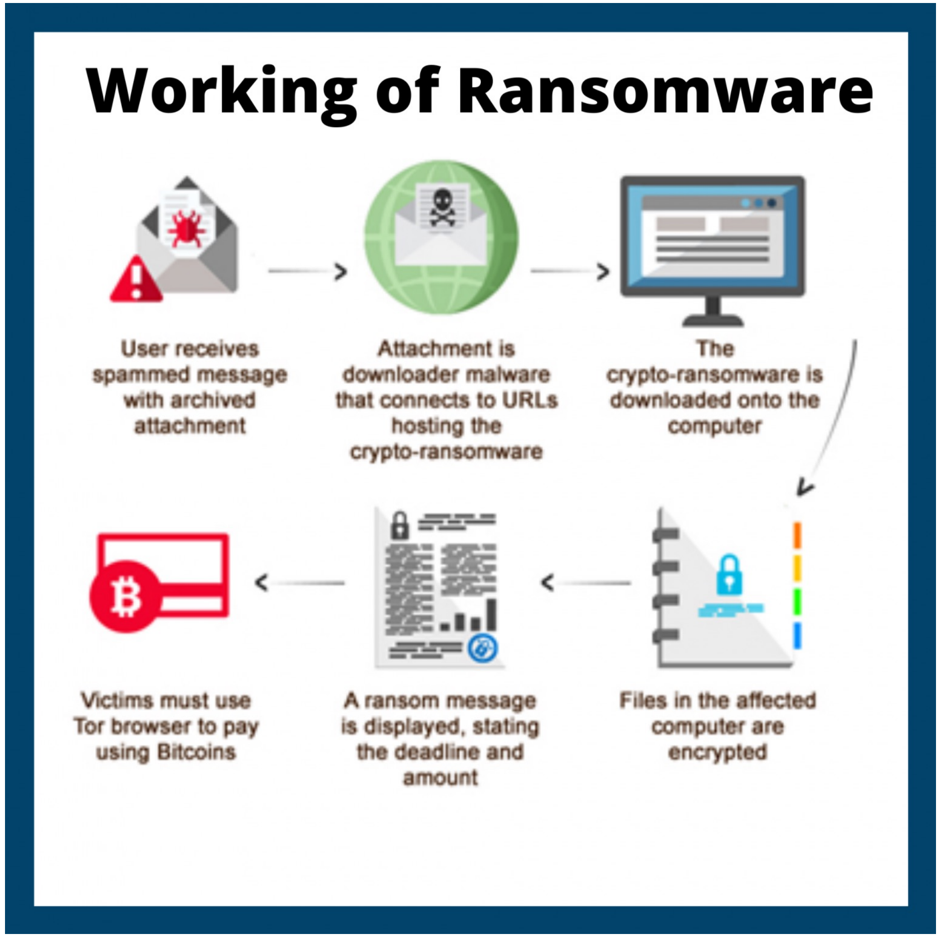
WHERE DO THE BREACHES OCCUR?



© HIPAA Journal 2022

UR COMPUTER IZ LOCKED
UNTIL U GIVES ME TREATS.
imgflip.com

RANSOMWARE - #1 PROBLEM FOR HEALTHCARE



Working of Ransomware

User receives spammed message with archived attachment

Attachment is downloader malware that connects to URLs hosting the crypto-ransomware

The crypto-ransomware is downloaded onto the computer

Files in the affected computer are encrypted

A ransom message is displayed, stating the deadline and amount

Victims must use Tor browser to pay using Bitcoins

RANSOMWARE

- 66% of surveyed healthcare organizations said they had experienced a ransomware attack in 2021, up from 34% in 2020 and the volume of attacks increased by 69%, which was the highest of all industry sectors.
- On average, after paying the ransom, healthcare organizations were only able to recover 65% of encrypted data, down from 69% in 2020. In 2020,
- 8% of healthcare organizations recovered all of their data after paying the ransom. That figure fell to just 2% in 2021.
- The global average across all industry sectors was $812,000. The ransom cost was lower in healthcare, but the overall cost of recovery was second-highest, with the total cost of a ransomware attack $1.85 million, which is considerably higher than the global average of $1.4 million.
- 97% of healthcare organizations that had cyber insurance that covered ransomware attacks said the policy paid out, with 47% saying the entire ransom payment was covered by their cyber insurance provider; however, obtaining cyber insurance to cover ransomware attacks is getting much harder due to the extent to which the healthcare industry is being targeted.

HEALTH CARE SYSTEMS AND THEIR COMPUTER SECURITY CONCERNS

A health system as an organization that includes:

- at least one hospital and
- at least one group of physicians that
- provides comprehensive care (including primary and specialty care)
- who are connected with each other and with the hospital through common ownership or joint management.

Note: Hospitals that employ community-based physicians who provide comprehensive care (but are not organized as a medical group) are considered health systems under this definition.

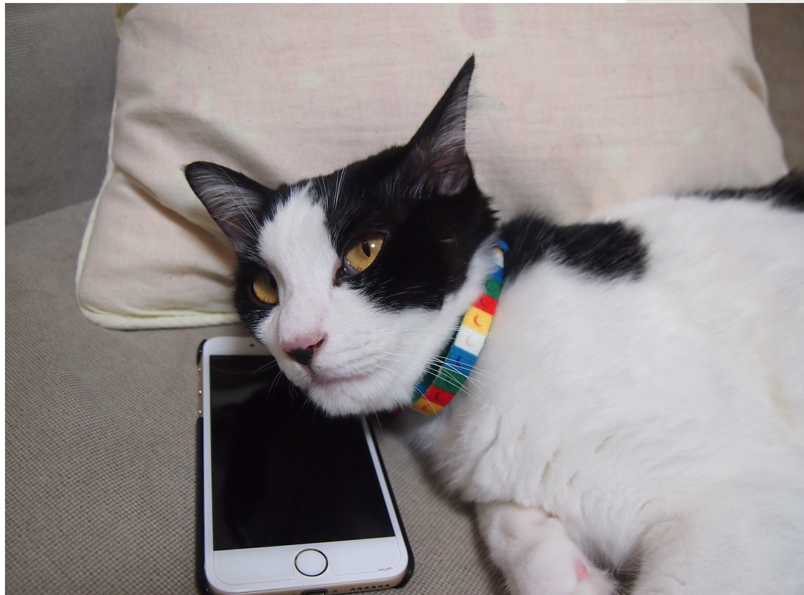
https://www.ahrq.gov/chsp/defining-health-systems/index.html

2. HEALTH CARE SYSTEM COMPUTERS AND INFORMATION

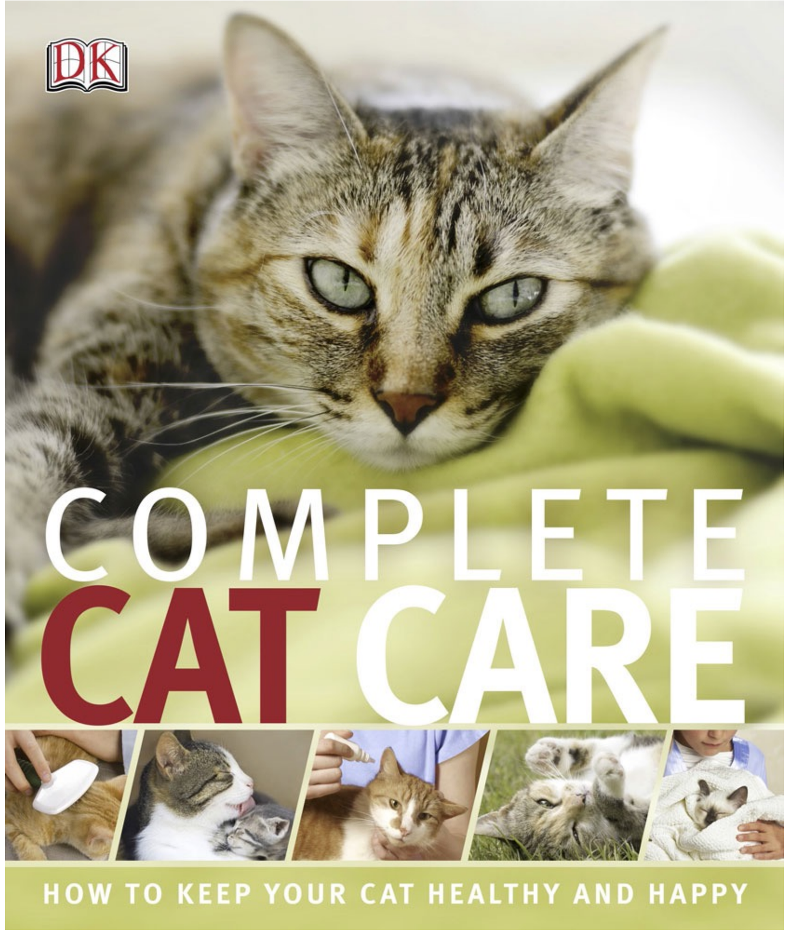
- Deployment – installed, mobile, cloud, web-based
- Charting – Patient records
- Compliance Tracking
- E-Prescribing
- Meaningful Use Certified
- ONC-ATCB Certified
- Self Service Portal

DEPLOYMENT

- Installed – the software is securely built into the system in some way
- Devices – watches, heart beat, blood pressure, …
- Mobile Devices – cell phones, cellular and wireless
- Laptops – mobile, storage, wireless and ethernet connections
- Desktops – not easy to move, storage, ethernet connections



GOAL COMPLETE ~~CAT CARE~~ HEALTH CARE



MEDICAL CHARTING

- **Demographics:** Name, age, contact and other details
- **Medications:** Current and previous
- **Allergies:** Including any potential drug-to-allergy interactions
- **History:** Comprehensive overview of a patient’s prior visits, ongoing conditions, medications and other factors
- **Family History:** Immediate family’s health, causes of death, common diseases
- **Surgical History:** Operations, dates, reports/results
- **Social History:** Occupations (current and past), community life and more
- **Developmental History:** Motor skills, cognitive, social/emotional, language, growth charts
- **Obstetric History:** Number of pregnancies, outcomes, complications
- **Immunization Records:** Vaccination dates
- **Habits:** Drug use, smoking/drinking, sexual history, lifestyle

WHO HAS ACCESS?

- The patient and the health care professionals directly involved in that patient’s care and treatment should be allowed access.
- Medical charts belong to the patient, who has the right to make sure their chart is accurate — if they find inaccuracies, they can petition their providers to make changes to their chart to ensure more accurate medical records.

BENEFITS

Completeness of patient information . EHR/EMR systems alert health care professionals of any missing, incomplete and inaccurate medical charts.

- Electronic health record (EHR) is a more longitudinal collection of the electronic health information of individual patients or populations.
- Electronic medical record (EMR) is a patient record created by providers for specific encounters in hospitals and ambulatory environments and can serve as a data source for an EHR.
- Personal health record (PHR) is an electronic application for recording personal medical data that the individual patient controls and may make available to health providers.

BENEFITS

- Patient information can be shared between doctors, specialists and even different departments. Everything is digitally stored and available on demand including patient histories, known allergies, previous procedures, used medications, test results...
- By simply logging in to the system, a specialist can instantly gain access to an online medical chart without having to wait for it to be delivered or faxed. Alternatively, paperwork incurs a possibility of misplacing information.
- Physicians can also easily sort through information using keywords or terms, which allows them to quickly locate the information they're looking for instead of sorting through multiple pages of records.

IMPROVED DIAGNOSIS AND TREATMENT

- Improves the diagnosis and treatment of patients
- Standardization of information, forms, etc
- Reduces the number of errors
- Avoids handwriting/legibility issues
- Reduces storage space
- Include health analytics and population health tools to help health care professionals improve the quality of care.

A PROBLEM WITH PAPER RECORDS

SECURITY OF RECORDS COMPARISON

ELECTRONIC

- Recovery database
- Ransomware
- Power failure
- Access control – need to know
- Check summed to ensure completeness
- Accessible, perhaps over Internet
- Needs electronic identity control, passwords or authentication devices
- Centralized system is a vulnerability
- Can be shared easily without concern
- Can be encrypted for privacy

PAPER

- Fire
- Flood
- Misplaced
- Illegibility
- Lost
- Stolen
- Tampered
- Images difficult to store
- Storage lock
- File cabinet is a vulnerability
- Copying may be unreliable

COMPLIANCE TRACKING

Abiding by all legal, professional, and ethical compliance standards in healthcare.

Healthcare, in general, is monitored by the

- Joint Commission which accredits hospitals. and
- HIPAA in healthcare.

COMPLIANCE TRACKING JOINT COMMISSION

- The Joint Commission is a United States-based nonprofit tax-exempt 501(c) organization that accredits more than 22,000 US health care organizations and programs. www. https://www.jointcommission.org/
- The international branch accredits medical services from around the world.
- A majority of US state governments recognize Joint Commission accreditation as a condition of licensure for the receipt of Medicaid and Medicare reimbursements.
- All member health care organizations are subject to a three-year accreditation cycle, and laboratories are surveyed every two years. The organization does not make its hospital survey findings public. However, it does provide the organization's accreditation decision, the date that accreditation was awarded, and any standards that were cited for improvement. Organizations deemed to be in compliance with all or most of the applicable standards are awarded the decision of Accreditation.

COMPLIANCE TRACKING
HIPPA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996)

1. modernized the flow of healthcare information
2. stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft
3. addressed some limitations on healthcare insurance coverage.
4. generally prohibits healthcare providers and healthcare businesses, called *covered entities*, from disclosing protected information to anyone other than a patient and the patient's authorized representatives without their consent.

COMPLIANCE TRACKING HIPPA TITLES

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
- Title III sets guidelines for pre-tax medical spending accounts, Title IV sets guidelines for group health plans, and
- Title V governs company-owned life insurance policies.

CYBERSECURITY COMPLIANCE CHALLENGES

- An ever-changing threat landscape
- Increasing sophistication and frequency
- Rapid technology evolution
- The skills gap
- The perimeterless organization
- Multiple regulations

Regulation

FIXES TO THE COMPLIANCE CHALLENGE

Many regulations focus on the same or similar threats and vulnerabilities and, therefore, entail similar mitigation requirements, for example:

- Establishing a governance framework for assuring cybersecurity accountability
- Identifying the systems that require greater security controls
- Monitoring data systems for attempted and successful breaches
- Implementing incident response programs that include notifying regulators and affected parties
- Testing the security program on a regular basis

INFORMATION RESOURCES

- Health Care Systems https://www.ahrq.gov/chsp/defining-health-systems/index.html
- https://www.cms.gov/CCIIO/Resources/Files/webportal
- www.hhs.gov/hipaa/for-professionals/privacy/index.html
- Biggest Health Care Data Breaches 2021 https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021
- Zero Trust Architectures https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

E-PRESCRIBING

The computer-based electronic generation, transmission, and filling of a medical prescription, taking the place of paper and faxed prescriptions with features including:

- Patient's identification
- complete active medication list
- Patient historical data
- Prescribe or add new medication and select the pharmacy where the prescription will be filled.
- Work with an existing medication within the practice
- Conducting all safety checks using an integrated decision support system, known as a Drug Utilization Review.
- Flagging availability of lower cost alternatives (if any)
- Providing information on formulary or tiered formulary medications, patient eligibility, and authorization requirements received electronically from the patient's insurance provider
- System integration capabilities (e.g., connection with various databases, connection with pharmacy and pharmacy benefit manager systems)

BENEFITS

- Reduce prescribing and dispensing errors
- Decrease the work needed to execute a prescription
- Speed receipt of prescribed drugs
- Avoid more adverse drug interactions and reactions
- More reliably offer to substitute less expensive drug alternatives by checking the formulary of the insurance provider in the doctor's office
- Improve medication compliance (taking the prescribed medications on time) by reducing lost and unfilled prescriptions and minimizing patient costs
- Reduce the incidence of drug diversion (drug abuse) by alerting providers and pharmacists of duplicative prescriptions for controlled substances.

Safety improvements are highly desirable; in 2000, the Institute of Medicine identified medication errors as the most common type of medical error in health care, estimating that this leads to several thousand deaths each year.

CYBERSECURITY ISSUES

- Hardware and software selection
- Erroneous alerts
- Integrity of data input
- Privacy of patient information stored in electronic format may lead to the possibility of novel errors, such as inadvertently divulging protected health information on the Internet through inadequate security practices.
- Instances of negligence may also arise, where employees may forward prescriptions to organizations outside its intended use.
- Verification of electronic signatures, in ensuring the medical integrity of the prescriptions received by pharmacists.
- Hospitals, clinics, and pharmacies are counselled to be protected with firewalls, use strict computer permission settings, and remain vigilant toward signs of an intrusion.
- System downtime
- Patient Access Lost
- Natural disasters

Thank you!!