Incorporating Cybersecurity into Telemedicine

Reese Weber, MBA, CISSP

Information Systems Security Officer

Indian Health Service, California Area Office

Learning Objectives

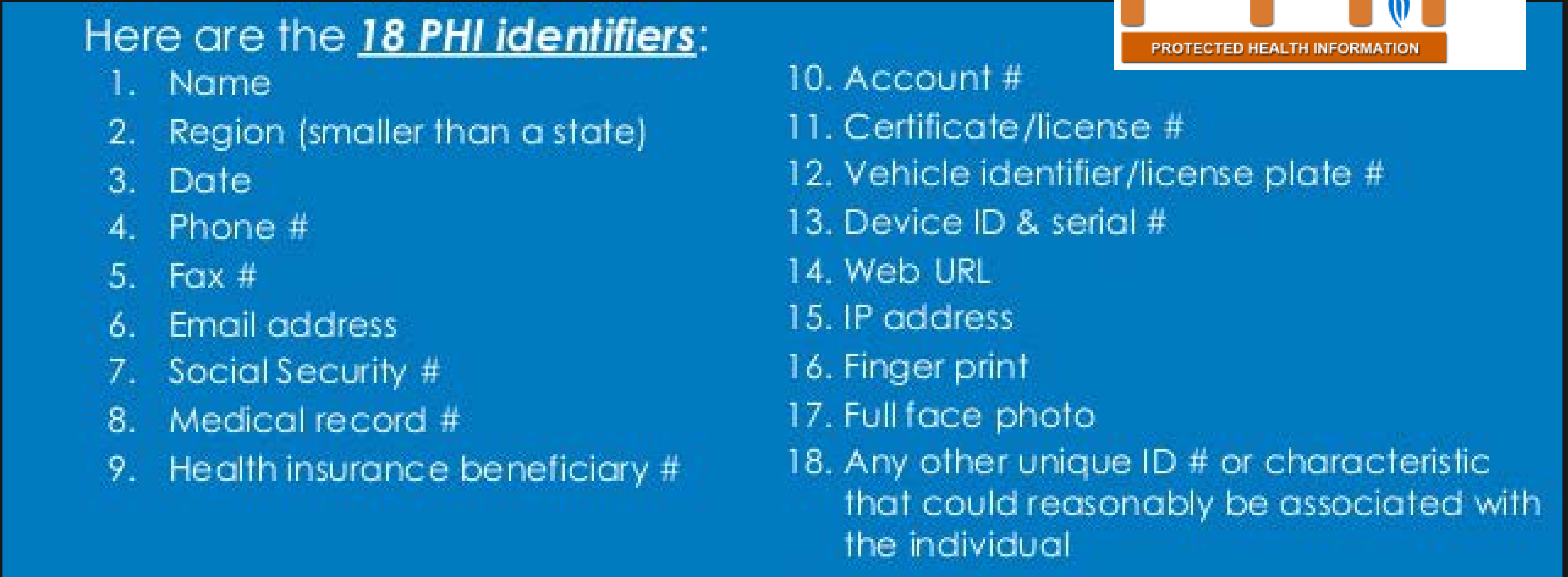
- Telemedicine and HIPAA Security Rule Compliance
- Security and Privacy Risks and Considerations
- Protecting Health Data in Telehealth

The HIPAA Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

HIPAA
Health Insurance Portability
and Accountability Act

The 18 HIPAA Identifiers



Here are the ***18 PHI identifiers***:

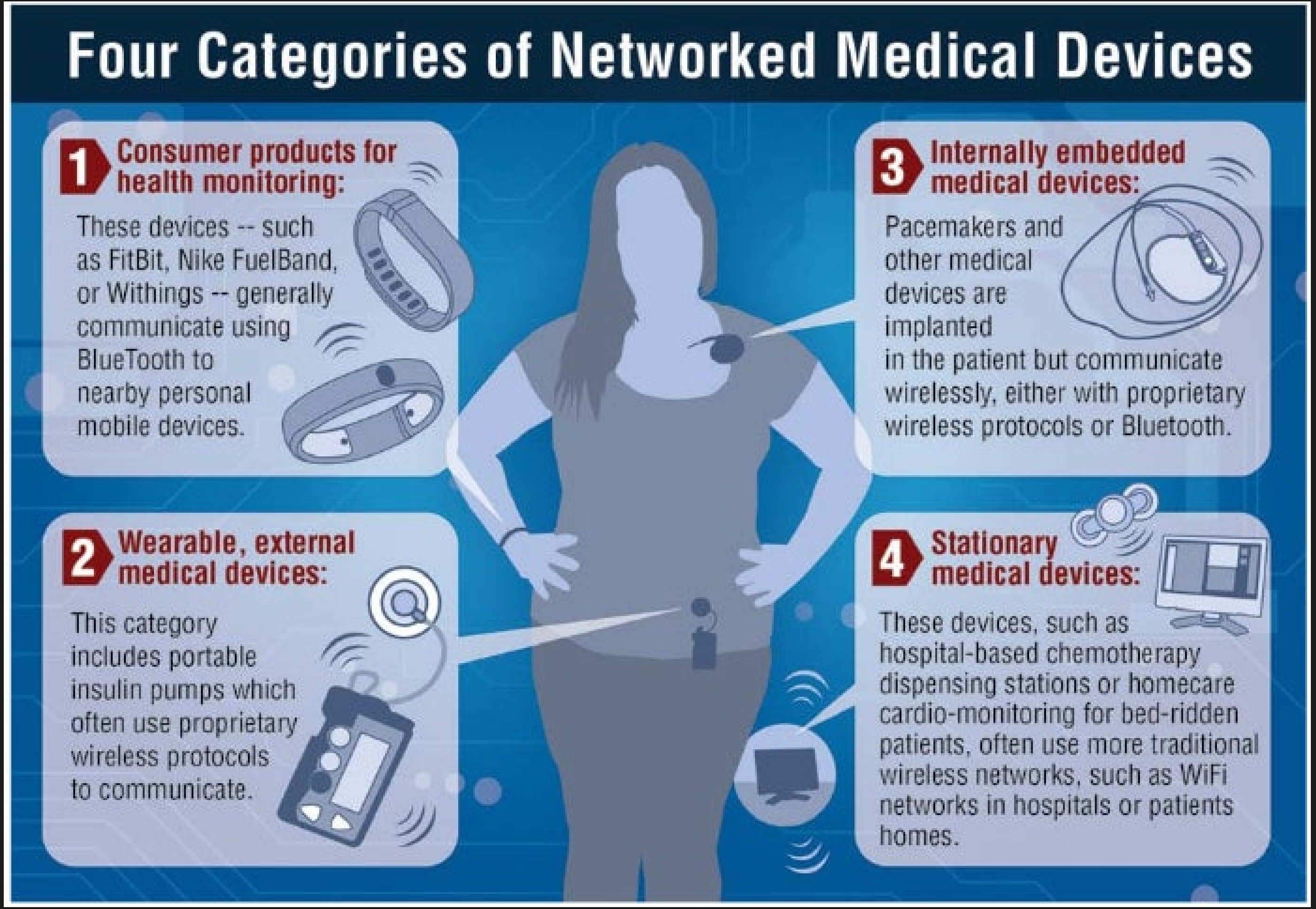
1. Name
2. Region (smaller than a state)
3. Date
4. Phone #
5. Fax #
6. Email address
7. Social Security #
8. Medical record #
9. Health insurance beneficiary #
10. Account #
11. Certificate/license #
12. Vehicle identifier/license plate #
13. Device ID & serial #
14. Web URL
15. IP address
16. Finger print
17. Full face photo
18. Any other unique ID # or characteristic that could reasonably be associated with the individual

Security and Privacy Risks & Considerations

- Device Security
- Patient Identification AND Provider Identification
- Access Security

Device Security

- Medical Device Security
- Providers device security (network, computers, data encryption)
- Patient’s security (network, home computer, etc)



Four Categories of Networked Medical Devices

1 Consumer products for health monitoring:

These devices -- such as FitBit, Nike FuelBand, or Withings -- generally communicate using BlueTooth to nearby personal mobile devices.

2 Wearable, external medical devices:

This category includes portable insulin pumps which often use proprietary wireless protocols to communicate.

3 Internally embedded medical devices:

Pacemakers and other medical devices are implanted in the patient but communicate wirelessly, either with proprietary wireless protocols or Bluetooth.

4 Stationary medical devices:

These devices, such as hospital-based chemotherapy dispensing stations or homecare cardio-monitoring for bed-ridden patients, often use more traditional wireless networks, such as WiFi networks in hospitals or patients homes.

Provider Identification

Examples of authentication factors

- If people can pose as doctors and scam people in real life, what do you think are the implications in telemedicine?
- What assurances can you make to your patients that your providers are identified and authenticated in **every session**?

Patient Identification

- Prevent accidental disclosure of health data
  - Sharing the wrong information or someone else’s personal health information with patient
- Prevent Fraud
  - An individual pretending to be the patient in an effort to obtain health services
  - A criminal impersonating the patient to gain access to private health information

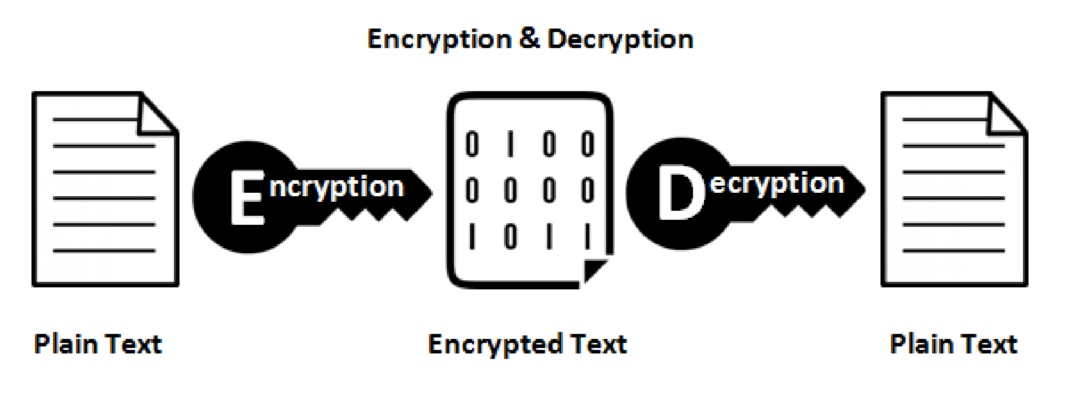
Personal Health Information (PHI) Technical Safeguards

Transmission Security - The security of ePHI during transmission should be established by the use of data encryption. ePHI should be rendered “unreadable, undecipherable or unusable” so that any patient healthcare or payment information is of no use to an unauthorized third party.

Photo courtesy of the IHS Telebehavioral Health Center of Excellence

Encryption

Encryption is the process of making data unreadable to anyone without the key, which is generally a password.



HIPAA
Health Insurance Portability
and Accountability Act

Although the HIPAA security rule does not explicitly require encryption, it requires “adequate protection” – which in today’s technology, equates to encryption.

Myth vs Fact

“I don’t have to worry about protecting this information because it has no value. What would a “bad guy” want with someone’s health information?”

- Credit card numbers go for $1 - $2 each on the black market.
- PHI sells for $20 - $200, depending on the type of patient data.

Business Associate Agreement (BAA)

Business Associates assist with or perform on behalf of a covered entity, a function or activity regulated by HIPAA.

Business Associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, billing or the ***provision of data storage or hosting services.***

Covered entities engaging in business transactions with Business Associates - who will encounter PHI in the course of the business transaction - **must** ensure that a “Business Associate Agreement” is in place **before any PHI** is provided or accessed by the Business Associate

State Law to Consider

- Confidentiality of Medical Information Act (CIMA)
  - Law recently amended to expand its scope to include health app developers
  - Health App Developers and PHR vendors are required to “Maintain the same standards of confidentiality required of a provider of health care

References and Links

- https://www.hipaajournal.com/hipaa-encryption-requirements/
- https://www.hhs.gov/hipaa/for-professionals/security/index.html
- https://healthitsecurity.com/news/telemedicine-privacy-security-considerations-for-providers
- https://www2.idexpertscorp.com/knowledge-center/single/healthy-privacy-and-security-practices-for-telemedicine
- https://www.ama-assn.org/sites/default/files/media-browser/public/arc-public/telemed-policy.pdf
- http://amberhawk.typepad.com/amberhawk/2011/05/cartoon-with-recent-data-losses-in-mind.html
- https://securityledger.com/2015/03/intel-new-approach-needed-to-secure-connected-health-devices/
- http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.06.&lawCode=CIV
- http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370