VIGITRUST

Global Advisory Board

Protecting Health Information

Protecting Health Information

- What is Health Information
- Laws & Regulations
- Main areas
- NIST / SANS frameworks
- Final thoughts

VIGITRUST
Global Advisory Board

What is Health Information

- Personal Identifiable Information (PII)
- Physical, mental or sexual health
- Medical history
- Laboratory results
- Insurance information

Laws & Regulations

HIPAA – Protected Health Information
GDPR – All sensitive personal data
CFR Part 11 – security features that limit user access and their privileges
ISO 27001 - international standard for information security

*OWASP - freely-available articles, methodologies, documentation, tools, and technologies

Main areas

Infrastructure – physical access to servers, mobile phone, wearables, and other devices containing health information

Software - firewalls, encryption, masking, de-identification, anonymization, authentication, authorization

People / Administrative - safety awareness training, policies that limit data access to certain people

NIST / SANS frameworks

Identify – context and risks, will help prioritizing efforts (risk matrix)

Protect – limit or contain the impact of a breach (implement strategies and policies)

Detect – being able to quickly identify the occurrence (logs and alerts)

Respond – contain the impact and communicate

Recover – plans for resilience and to restore the systems (backups and recovery)

Final thoughts

Nowadays we protect Data

Cybersecurity is a never ending battle

Keep training people

Keep improving all the technical aspects

Do, Test, Review

VIGITRUST
Global Advisory Board