MCGLOBALTECH

BRIDGING THE GAP BETWEEN MISSION, TECHNOLOGY & SECURITY

Best Practices for Implementing PHI Security

Healthcare Compliance Symposium 2019

April 4, 2019

Presenter

- **William J McBorrough**, MSIA, CISSP, CISA, CRISC
- Chief Security Advisor, **MCGlobalTech**
- Assistant Professor, Cybersecurity, University of Maryland
- 20 years Information Security Professional
- 11 years Adjunct College Professor
- Security and Risk Management “Expert”

CISSP® Certified Information Systems Security Professional

CISA® Certified Information Systems Auditor® An ISACA® Certification

C|E|H™ Certified Ethical Hacker

CRISC™ Certified in Risk and Information Systems Control™ An ISACA® Certification

HITRUST CSF Certified

MCG

AGENDA

I. Framing the Healthcare Security Problem

II. Healthcare Security Trends in 2018

III. Implementing PHI Security: Threats and Best Practices

AGENDA

I.

Framing the Healthcare Security Problem

Security vs. Compliance

- Compliance - Conforming to a set of standards. Generally confirmed by an assessor providing an opinion-based observation, inquiry, and inspection. Just a matter of focus

- Security – Implementing risk-based Administrative, Physical and Technical controls to provide confidentiality, integrity, availability, accountability, assurance and privacy.

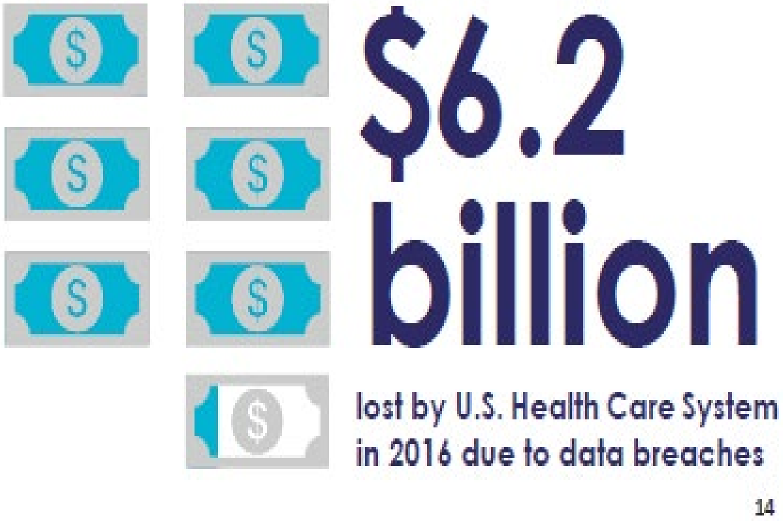
Motives for Stealing PHI (Why)

Most Common motive – MONEY.

– According to report by Price Waterhouse Cooper:

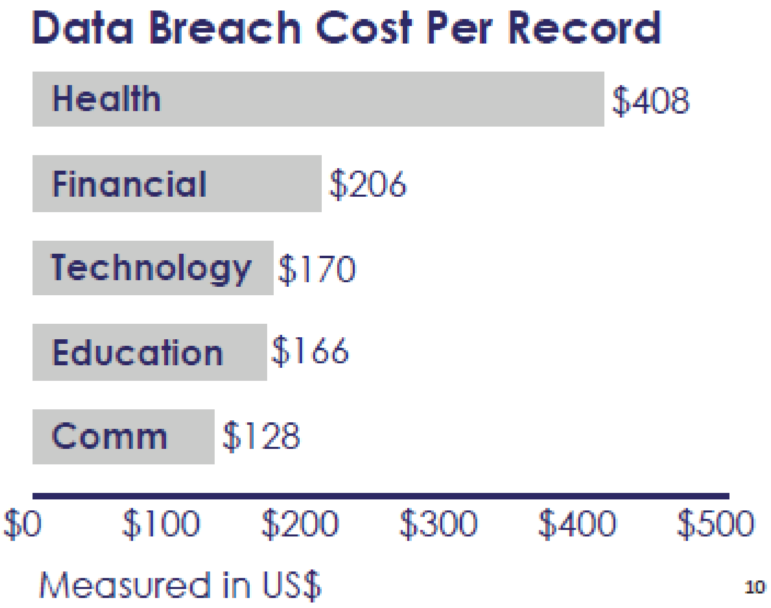
- Comprehensive Health Insurance Record (e.g. financial, medical, PII) is worth up to $1000 on black market.
- Basic health insurance credentials worth approx. $20 per record
- Compare to $1 per stolen credit card

Cost of Data Breaches



$6.2 billion

lost by U.S. Health Care System in 2016 due to data breaches [14]



Data Breach Cost Per Record

Measured in US$ [10]

$408 * 500 records = $204,000

Small Business Impacts

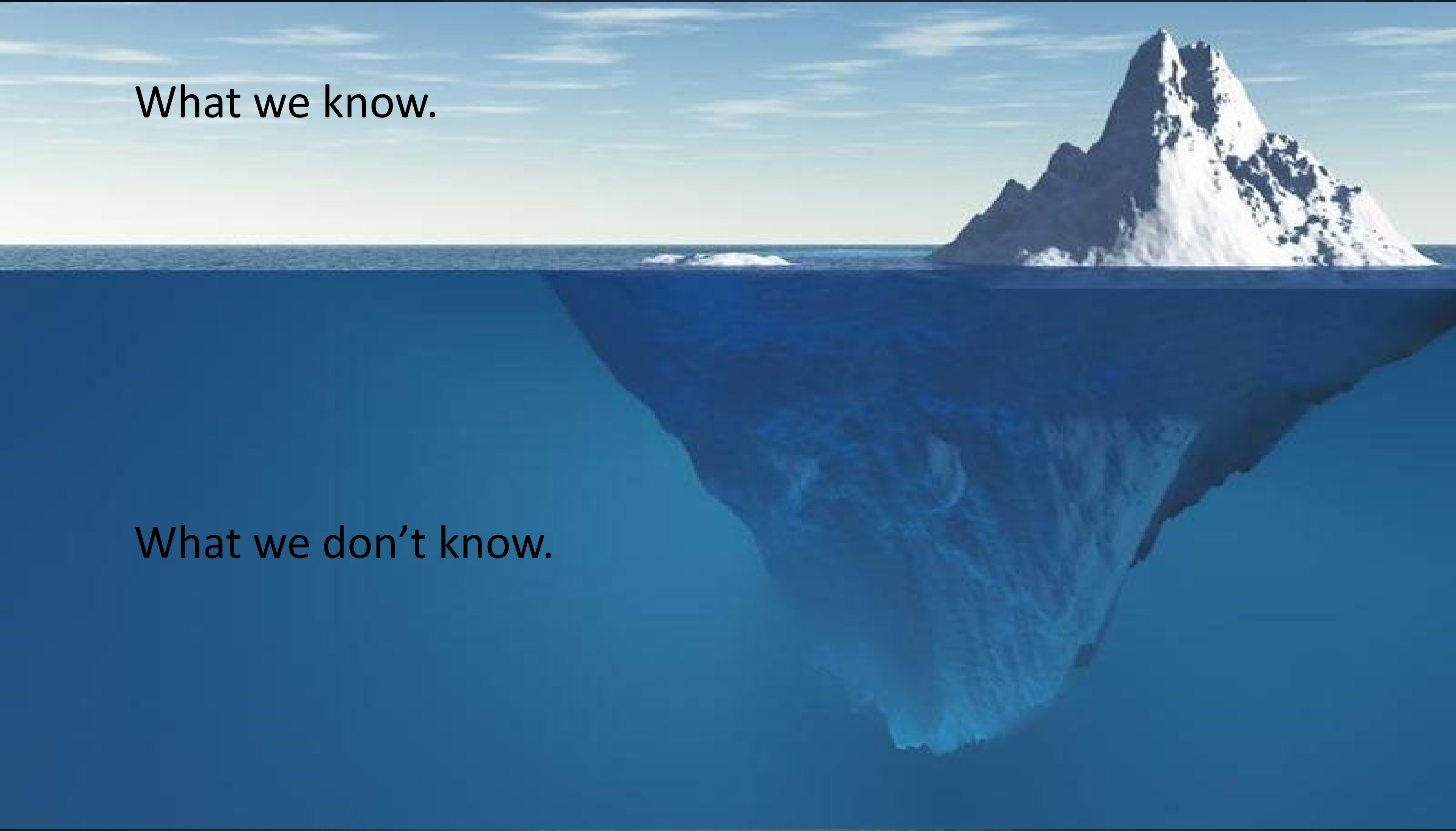
- 58% of malware attack victims are small businesses
- In 2017, cyber-attacks cost SMBs on average $2.2M
- 60% of small businesses go out of business within six months of an attack
- 90% of small businesses do not use any data protection at all for company and customer information

AGENDA

II.

Healthcare Security Trends in 2018

When it comes to Security Events



What we know.

What we don't know.

Healthcare Security Trends in 2018

- 15M+ Patient Records Breached in 2018
- At least one health data breach per day

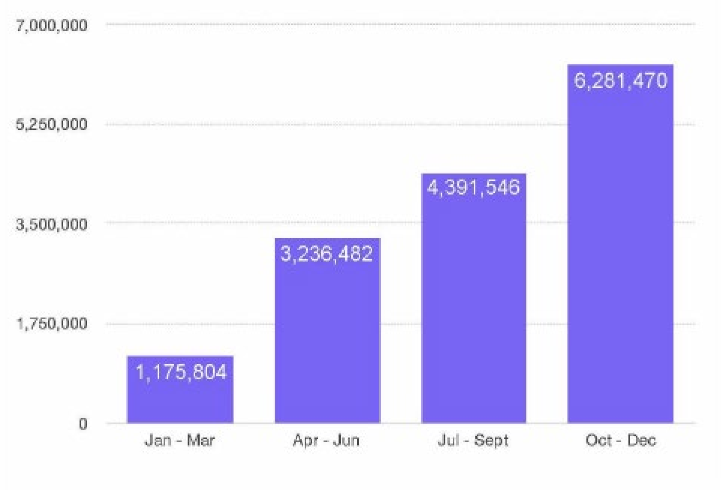
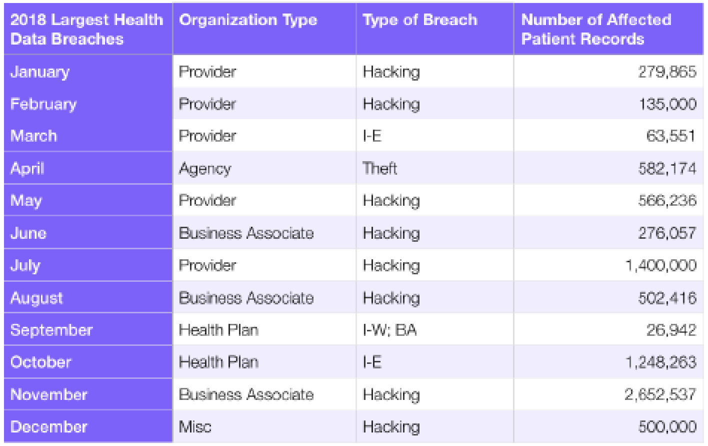


Figure 3. Affected patient records by quarter, 2018 health data breaches



2018 Largest Health Data Breaches	Organization Type	Type of Breach	Number of Affected Patient Records
January	Provider	Hacking	279,865
February	Provider	Hacking	135,000
March	Provider	I-E	63,551
April	Agency	Theft	582,174
May	Provider	Hacking	566,236
June	Business Associate	Hacking	276,057
July	Provider	Hacking	1,400,000
August	Business Associate	Hacking	502,416
September	Health Plan	I-W; BA	26,942
October	Health Plan	I-E	1,248,263
November	Business Associate	Hacking	2,652,537
December	Misc	Hacking	500,000

Figure 4. Largest incidents, 2018 health data breaches

Healthcare Security Trends in 2018

- 58% of healthcare systems breaches involve inside actors (**Insider Threat**)
- 70% of breach incidents involving malicious code were **Ransomware** infections
- Most commonly breached assets are databases (and paper documents)
- Basic security measures still not implemented (e.g. Lost/Stolen devices unencrypted)

Healthcare Security Trends in 2018

- Insider Snooping STILL a problem
- VCU Health System
- Employee inappropriately accessed patient data for 15 years
- January 3, 2003 to May 10, 2018

Healthcare Security Trends in 2018

- Singe largest breach: 2.65M patient records
- Atrium Health of North Carolina (BA)
- Compromised Information: DOBs, SSNs, Insurance Policy Information, Date of Service
- Medical/Financial Records Not Affected
- Week long access
- Hacker unable to download/remove data

Healthcare Security Trends in 2018

- Health Information and Management Systems Society
- 2018 HIMSS Cybersecurity Survey
- Feedback from Health Information Security Professionals
- 3 major observations

HIMSS

Healthcare Security Trends in 2018

- Observation 1: Healthcare organizations are making progress in improving their cybersecurity programs
  - Year over year increase in resources to address cybersecurity
  - Most organizations have dedicated/defined budget allocation
  - Most organizations are conducting risk assessments at least annually
  - Addressing supply chain risk

Healthcare Security Trends in 2018

- Observation 2: Healthcare Cybersecurity Programs could be improved in multiple areas
  - Biggest barrier: Personnel and financial resources
  - No universally adopted security framework
    - NIST, HITRUST, ISO, COBIT, Critical Security Controls
  - No uniform source of cyber threat intelligence
  - Formalized insider threat management program needed
  - More frequent and comprehensive penetration testing
  - Human Safeguards: Testing and Training

Healthcare Security Trends in 2018

- Observation 3: What's Next: Concerns and Priorities
  - Breaches, Ransomware, Credential Stealing Malware
  - Medical Device Security
  - Concerns about disruption and failure of other critical infrastructure services

AGENDA

III.

Implementing PHI Security: Threats and Best Practices

Health Industry Cybersecurity Practices

- Background
  - Cybersecurity Act of 2015
  - Section 405(d) – Aligning Healthcare Industry Security Approaches
  - 405(d) Task Group
  - December 28, 2018 publication

- ***Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients ("HICP")***
  - *Best Practices consistent with the NIST Cybersecurity Frameworks*

Health Industry Cybersecurity Practices

- **HICP: Main Document**
  - Discusses current top threats facing healthcare industry
  - Raise general awareness of security issues
  - Call to Action
- **HICP: Technical Volume I**
  - Discusses ten cybersecurity best practices for small health care organizations
- **HICP: Technical Volume II**
  - Discusses ten cybersecurity best practices for medium-sized and large health care organizations
- **HICP: Resources and Templates Volume**
  - Provides additional resources and references

Health Industry Cybersecurity Practices

- Task Group identified **Top Five Threats** facing Industry

  I. E-mail phishing attacks

  II. Ransomware attacks

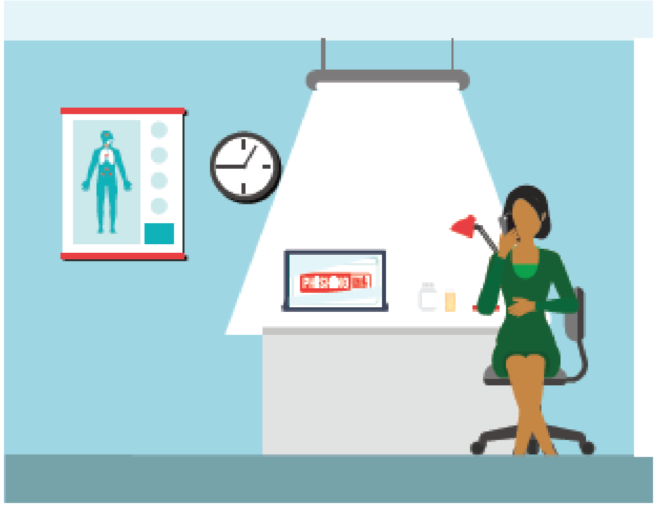
  III. Loss or theft of equipment or data

  IV. Insider, accidental or intentional data loss

  V. Attacks against connected medical devices that may affect patient safety

Health Industry Cybersecurity Practices

- E-mail phishing attacks
  - Vulnerabilities
    - Lack of awareness training
    - Lack of email security tools
  - Impact
    - Loss of reputation
    - Loss of PHI
    - Patient safety impact



Health Industry Cybersecurity Practices

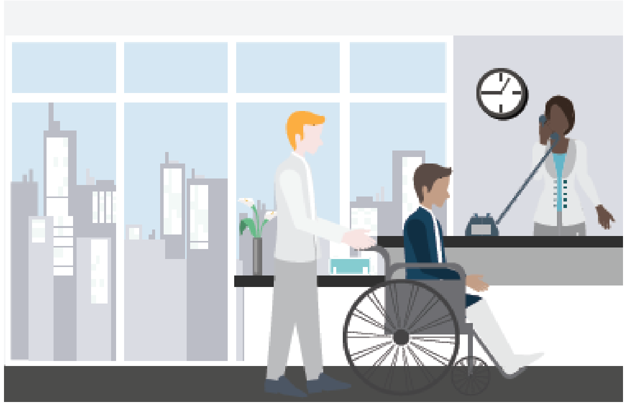
- Ransomware attack
  - Vulnerabilities
    - Lack of data backup
    - Unpatched software
    - Lack of anti-malware tools
  - Impact
    - Service disruption
    - Expense of recovery
    - HIPAA "Security incident"
    - Patient safety impact

Health Industry Cybersecurity Practices

- Loss or Theft of Equipment or Data
  - Vulnerabilities
    - Lack of physical security
    - Lack of encryption
    - Lack of awareness
  - Impact
    - Service disruption
    - Inappropriate access to PHI
    - HIPAA “Security incident”
    - Lost productivity
    - Patient notification

Health Industry Cybersecurity Practices

- Insider Threat Incidents
  - Vulnerabilities
    - Lack of PHI monitoring
    - Lack of training
    - Lack of DLP tools
  - Impact
    - Loss of PHI
    - Breach reporting and notifications
    - Financial loss
    - Patient safety impact

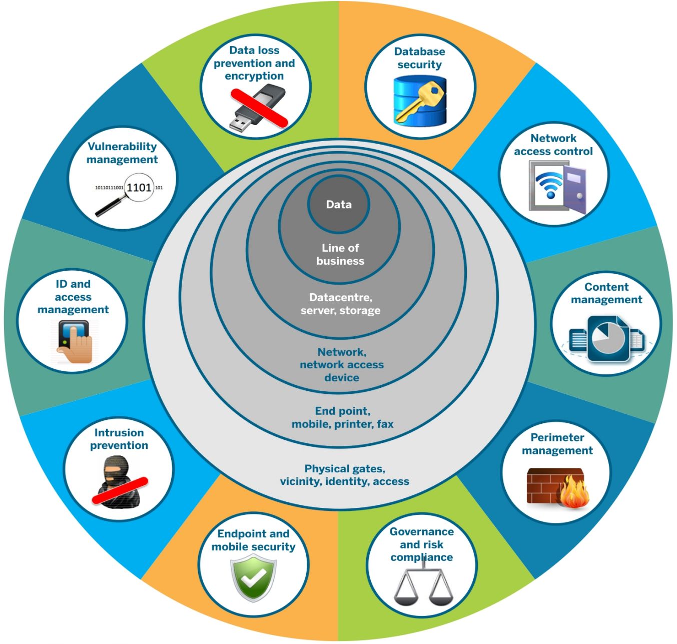


Health Industry Cybersecurity Practices

- Medical Device attacks
  - Vulnerabilities
    - Lack of monitoring
    - Unpatched software
    - Legacy equipment
  - Impact
    - Service disruption
    - Device Malfunction
    - Patient safety impact

HICP Best Practices

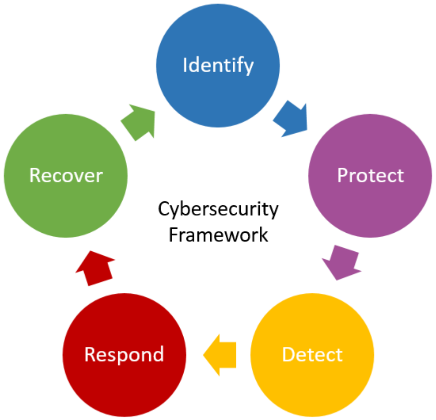
- **Ten Best Practices to Mitigate Threats**
  1. E-mail protection system
  2. Endpoint protection systems
  3. Access Management
  4. Data protection and loss prevention
  5. Asset Management
  6. Network Management
  7. Vulnerability Management
  8. Incident Response
  9. Medical Device Security
  10. Cybersecurity policies


Data loss prevention and encryption
Database security
Network access control
Content management
Perimeter management
Governance and risk compliance
Endpoint and mobile security
Intrusion prevention
ID and access management
Vulnerability management
1101
Data
Line of business
Datacentre, server, storage
Network, network access device
End point, mobile, printer, fax
Physical gates, vicinity, identity, access

NIST Cybersecurity Framework

NIST "Framework for Improving Critical Infrastructure Security" Cybersecurity Framework v.1 released February 2014.

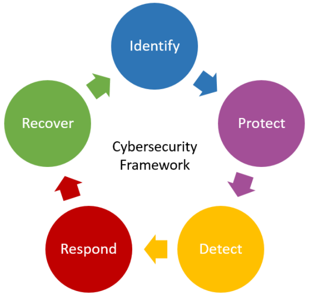
- 98 Best Practices for Managing [Security] Risks
- Common Language to discuss Security
- Not a compliance checklist



NIST CSF and HIPAA Security Rule crosswalk released by OCR in February 2016

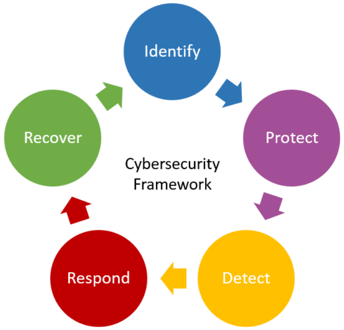
"…improve compliance with HIPAA Security Rule and better protect patient data." - OCR

Identify – Set Strategy to Manage Risk



- Asset Management
  - Document and track all PHI and supporting systems
- Business Environment
- Governance
  - Develop a security and policy that reflects HIPAA and HITECH requirements
- Risk Assessment
  - Assess and measure security and privacy risks to PHI
- Risk Management Strategy
  - Determine priorities and tolerance. Ensure they are reflected in operations
- Supply Chain Risk Management
  - Implement Business Associates Agreements. Monitor them for Vendor compliance

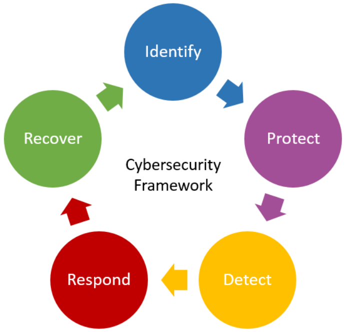
Protect – Implement Controls to Safeguard PHI



- Identify Management and Access Control
  - Implement technology to restrict access to authorized authenticated users.
- Awareness and Training
  - Deliver role-based training on PHI security and privacy. Provide ongoing awareness to encourage secure behavioral practices.
- Data Security
  - Implement technology to encrypt PHI in storage, transit and processing
- Information Protection Processes and Procedures
  - Develop policy framework that reflects HIPPAA and HITECH compliance requirements
- Maintenance
  - Develop maintenance and repair capabilities for systems that support PHI
- Protective Technology
  - Implement technology to secure PHI

Detect – Ensure Timely Awareness of Events

- Anomalies and Events
  - Implement technologies to ensure timely awareness of events that potentially pose risk to PHI

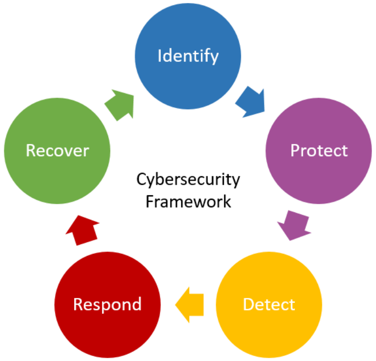


- Security Continuous Monitoring
  - Implement technologies to monitor systems that store and process PHI to identify security events and verify effectiveness of security safeguards

- Detection Processes
  - Develop processes and procedures to ensure timely awareness of events that potentially pose risk to PHI

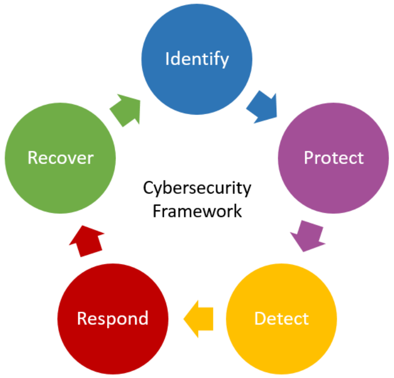
Respond – React to Detected Events

- Response Planning
  - Develop processes and procedures to ensure timely response to detected events that impact PHI
- Communications
  - Coordinate with internal and external stakeholders
- Analysis
  - Investigate detected incidents
- Mitigation
  - Contain incidents affecting PHI
- Improvements
  - Incorporate lessons learned into future activities



Recover – Return to Normal Operations

- Recovery Planning
  - Develop plans for cyber resilience
  - Plan for timely restoration of PHI and dependent systems, networks and related processes.
  - Test your business continuity plans



- Improvements
  - Incorporate lessons learned into future activities

- Communications
  - Coordinate with internal and external stakeholders

Cyber Incident Reporting

HHS recommended Steps:

- Contact FBI Field Office Cyber Task Force www.fbi.gov/contact-us/field-offices
- Report incidents to US-CERT www.us-cert.gov/ncas and FBI’s Internet Crime Compliant Center www.ics.gov
- For healthcare-specific indicator sharing, contact HHS’s Health Sector Cybersecurity Coordination Center (HC3) at HC3@hhs.gov

References and Sources

- Protenus 2019 Breach Barometer Report
  www.protenus.com/2019-breach-barometer

- 2018 HIMSS Cybersecurity Survey
  www.himss.org/2018-himss-cybersecurity-survey

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

- Verizon 2018 Protected Health Information Data Breach Report
  https://enterprise.verizon.com/resources/reports/dbir/

- 2018 Cost of a Data Breach Study by Ponemom
  www.ibm.com/security/data-breach

About MCGlobalTech

MCGlobalTech

- Mission Critical Global Technology Group (MCGlobalTech) is a Information Risk Management and Cybersecurity Firm founded by industry leaders to provide strategic advisory and security consulting services to public and private sector business managers to better align technology and security programs with organizational mission and business goals.
- The Principals at MCGlobalTech have been providing Information Security services to the Federal Government and the private sector for over 25 years

Contact Us

MCGlobalTech
1325 G Street, NW
Suite 500
Washington, District of Columbia 20005
Phone: 202.355.9448
Email: Info@mcglobaltech.com
Web: www.mcgcyber.com

William J. McBorrough
Chief Security Advisor
wjm4@mcglobaltech.com
O: (202) 355-9448 x101
M: (571) 249-4677

Sales Division
Corporate Headquarters
sales@mcglobaltech.com
(202) 355-9448 x200

QUESTIONS