HealthTech

IT and Information Protection Strategy

Jay Kuo

TABLE OF CONTENTS

1 Introduction

2 IT Infrastructure & Asset

3 Emerging Technology Threat

4 My Proposed Framework

5 Alignment of IT Strategy with Business Objectives

6 Conclusion

INTRODUCTION

Securing HealthTech’s Future in Telehealth

- Purpose of The Report
- Key Findings
- Recommendations

INTRODUCTION

Securing HealthTech's Future in Telehealth

- Purpose of The Report

The CAGR forecast for telehealth market between 2023 to 2030 is

19.7%

- Key Findings

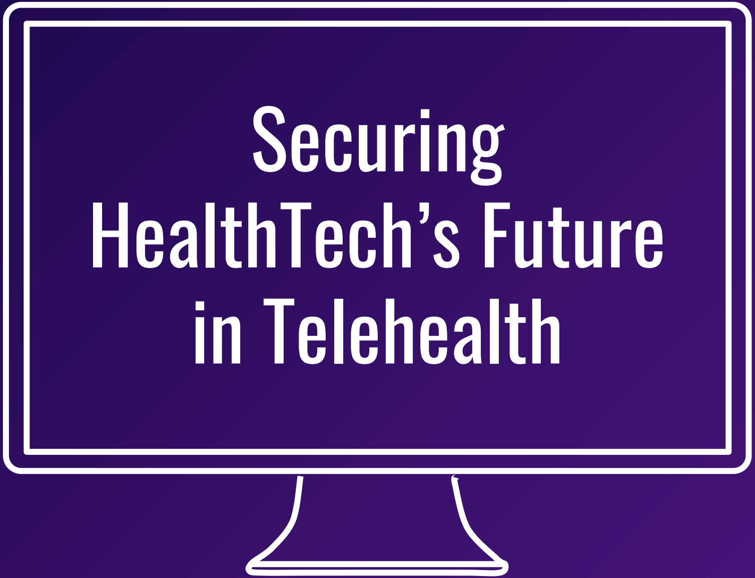
INTRODUCTION

Securing HealthTech's Future in Telehealth

- Purpose of The Report
- Key Findings
  - Deepfake
  - AI-Driven Phishing Attack
  - IoT Device Vulnerabilites
- Recommendations

INTRODUCTION

- Purpose of The Report
- Key Findings
- Recommendations



Securing HealthTech's Future in Telehealth

HIPAA + NIST

IT Infrastructure & Data Protection Essentials

DEFINITION OF TELEHEALTH

IT Infrastructure Components

Information Assets to Protect

IT Infrastructure & Data Protection Essentials

- Modern Healthcare Delivery
- Remote Consultations
- Digital Access to Care Services

DEFINITION OF TELEHEALTH

IT Infrastructure Components

Information Assets to Protect

IT Infrastructure & Data Protection Essentials

- Secure Network Connections
- Data Storage Solutions
- Communication Systems

DEFINITION OF TELEHEALTH

IT Infrastructure Components

Information Assets to Protect

IT Infrastructure & Data Protection Essentials

DEFINITION
OF
TELEHEALTH

IT
Infrastructure
Components

Information
Assets
to Protect

- Protected Health Information (PHI)
- Healthcare Provider Data
- E-Prescription and Treatment Plans

03

Emerging Technology Threats

Emerging Technology Threats

Deepfake Technology

AI-Driven Phishing Attacks

IoT Device Vulnerabilites

Emerging Technology Threats

- Impersonation of Patients or Providers
- Erosion of Trust
- Data Privacy and Security Risk

Deepfake Technology

AI-Driven Phishing Attacks

IoT Device Vulnerabilites

Emerging Technology Threats

- Enhanced Targeting and Personalization
- Automated and Scalable Attacks
- Bypassing Traditional Security Measures

Deepfake Technology

AI-Driven Phishing Attacks

IoT Device Vulnerabilites

Emerging Technology Threats

Deepfake Technology

AI-Driven Phishing Attacks

IoT Device Vulnerabilites

- Exploitation of Unsecured Devices
- Potential for Widespread Impact
- Challenges in Patching and Updating

04

My Proposed Framework

My Proposed Framework

My Proposed Framework

HIPAA + NIST

My Proposed Framework

RISK ASSESSMENT

HIPAA

Security Management Process

§ 164.308(a)(1)(ii)(A)

NIST

SP 800-30

Provides a comprehensive guide for conducting risk assessments, identifying vulnerabilities, potential threats, and impacts.

My Proposed Framework

AI-Phishing Training

HIPAA

Security Awareness and Training

§ 164.308(a)(5)

NIST

SP 800-50

Building an Information Technology Security Awareness

My Proposed Framework

IoT Device
Security Audits

HIPAA

Security Rule – Protection from Malware

§ 164.308(a)(5)(ii)(B)

NIST

SP 800-53

Security and Privacy Controls for Information Systems and Organizations

My Proposed Framework

Deepfake Incident Response

HIPAA

Security Incident Procedures

§ 164.308(a)(6)

NIST

SP 800-61

Computer Security Incident Handling Guide

My Proposed Framework

Monitoring
for
AI-Phishing

HIPAA

Information System Activity Review

§ 164.308(a)(1)(ii)(D)

NIST

SP 800-137

Information Security Continuous Monitoring for Federal Information Systems and Organizations

My Proposed Framework

IoT Device Recovery Planning

HIPAA

Data Backup Plan

§ 164.308(a)(7)(ii)(A)

NIST

SP 800-34

Contingency Planning Guide for Federal Information Systems

My Proposed Framework

Deepfake Risk Assessment

AI-Phishing Training

IoT Device Security Audits

Deepfake Incident Response

Monitoring for AI-Phishing

IoT Device Recovery Planning

My Proposed Framework

Deepfake Risk Assessment

AI-Phishing Training

IoT Device Security Audits

Deepfake Incident Response

Monitoring for AI-Phishing

IoT Device Recovery Planning

05

Alignment of IT Strategy with Business Objectives

Alignment of IT Strategy with Business Objectives

Enhancing Patient Trust
Risk Assessment

Ensuring Business Continuity
Security Audit

Regulatory Compliance
Incident Response Planning

Safeguarding Patient Data
Training and Monitoring

Facilitating Innovation
Adaptive Security Measures

Promoting Operational Efficiency
Proactive Threat Management

06

Conclusion

Conclusion

- Introduction of Telehealth
- Emerging Threats of Telehealth Industry
- Customized Framework
- The Alignment of Framework with Business Objectives

Conclusion

Impersonation of Patients or Providers

Erosion of Trust

Data Privacy and Security Risk

REFERENCE

- Fortune Business Insights. (2023, June 29). *Telehealth market size to surpass USD 504.24 billion in 2030, exhibiting a CAGR of 19.7%*. GlobeNewswire News Room. https://www.globenewswire.com/en/news-release/2023/06/29/2697018/0/en/Telehealth-Market-Size-to-Surpass-USD-504-24-Billion-in-2030- exhibiting-a-CAGR-of-19-7.html#:~:text=The%20market%20is%20projected%20to,%2C%20cardiology%2C%20and%20online%20consultation.
- Wani, T. A., Mendoza1, A., & Gray2, K. (n.d.). *Hospital bring-your-own-device security challenges and solutions: Systematic review of Gray Literature*. JMIR mHealth and uHealth. https://mhealth.jmir.org/2020/6/e18175
- Wikimedia Foundation. (2023, May 27). *Anthem Medical Data Breach*. Wikipedia. https://en.wikipedia.org/wiki/Anthem_medical_data_breach
- Sumsub. (2023, June 9). *New North America Fraud Statistics: Forced Verification and AI/Deepfake Cases Multiply at alarming rates*. https://sumsub.com/newsroom/new-north-america-fraud-statistics-forced-verification-and-ai-deepfake-cases-multiply-at-alarming-rates/
- Burgan, C. (2023, April 17). *NIST launching project to Mitigate Smart Tech Cyber Risks in Telehealth*. MeriTalk. https://www.meritalk.com/articles/nist-launching-project-to-mitigate-smart-tech-cyber-risks-in-telehealth/