LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Threat Modeling for Mobile Health Systems

04/30/2020

Report #: 202004301030

Agenda

- Introduction
- Threat Modeling Overview
- S.T.R.I.D.E
- S.T.R.I.D.E: Spoofing
- S.T.R.I.D.E: Tampering
- S.T.R.I.D.E: Repudiation
- S.T.R.I.D.E: Information Disclosure
- S.T.R.I.D.E: Denial of Service
- S.T.R.I.D.E: Elevating Privileges
- Authentication Threats
- Authorization Threats
- Privacy Threats
- Audit and Logging Threats
- References
- Questions

NCUA.gov

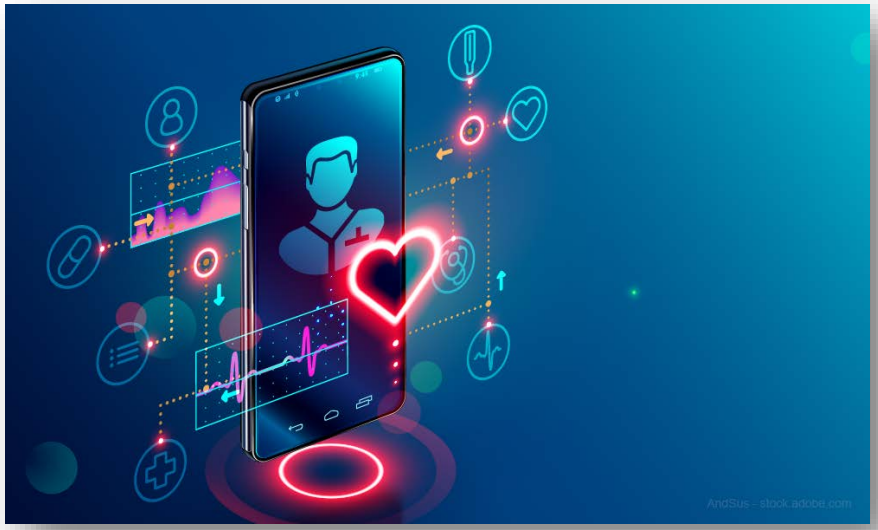
Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction

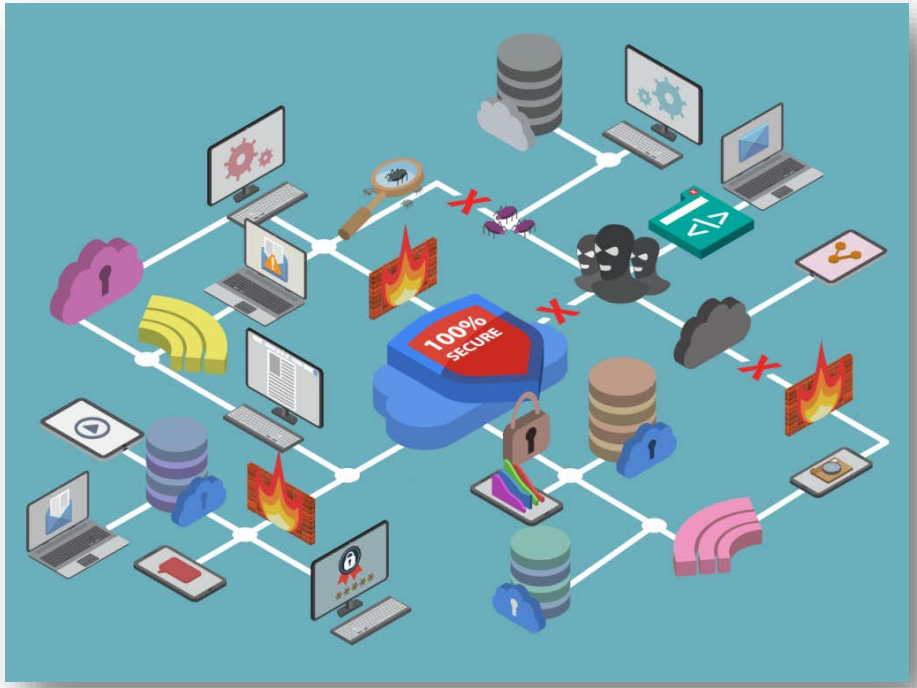
- Advances in mobile health (mHealth), respectively IoTHealth, are likely to reduce costs and improve the quality of healthcare.
- Although telehealth systems may improve the quality of healthcare, the digitalization of health records, the collection, evaluation and provisioning of patient data, and the transmission of patient data over public networks pose new privacy and security threats to patients and healthcare providers
- Threat modeling serves as a foundation for the analysis and specification of security requirements. It involves understanding of system complexity and identification of all possible threats to the system.



Managed Healthcare

Threat Modeling Overview

- Threat modeling is an important aspect of the security development lifecycle, which is a process aiming to build better and more secure systems or software.
- It is a technique, which aims to find assets, analyze potential threats and mitigate them. This provides defenders with important insights:
  - The most likely attack vectors
  - Assets an attacker is attracted to
  - Attack vectors that otherwise would have gone unnoticed



Paubox

Threat Model S.T.R.I.D.E

- STRIDE is an acronym that stands for 6 categories of security risks:
  - Spoofing
  - Tampering
  - Repudiation
  - Information Disclosure
  - Denial of Service
  - Elevation of Privileges
- Each category of risk aims to address one aspect of security.
- To follow STRIDE, you decompose your system into relevant components, analyze each component for susceptibility to the threats, and mitigate the threats.

Checkmarx

Threat Model S.T.R.I.D.E: Spoofing

Spoofing

- Spoofing refers to the act of posing as someone else (i.e. spoofing a user) or claiming a false identity (i.e. spoofing a process).
    - This category is concerned with **authenticity**.

mHealth Security Perspective: Attacker using user authentication information to access sensitive medical data

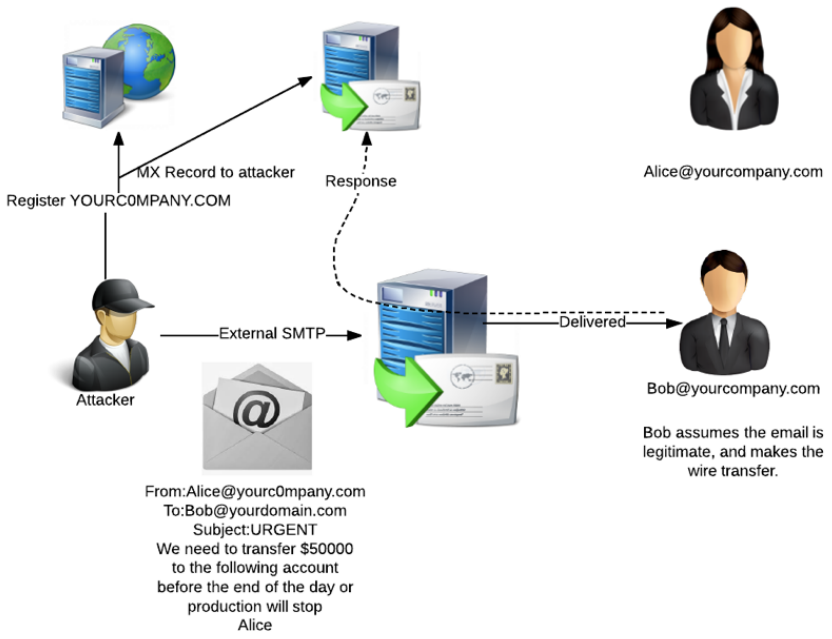
- Use of Email spoofing to lure patients into disclosing personal information or harvesting user credentials.
    - Commonly, the spoofed emails are sent modifying the sender name or email address. Also, sometimes the body of the message is formatted in such a way that it appears to be legitimate to the recipient.

Paubox

Threat Model S.T.R.I.D.E: Spoofing cont…

Mitigations/Countermeasures

- Strong authentication: User must be authenticated to the system using a strong password policy, biometrics or multi-factor authentication mechanisms.
- Encryption: All credentials must be encrypted, and it has to be ensured that credentials do not traverse the wire in clear text form. (S/MIME)
- Cryptographic protocols: Cryptographic protocols such as TLS/SSL must be used to ensure a secure (encrypted) communication between system components.
- **Email Spoofing**
  - Validation tools: Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting & Conformance (DMARC) used to create policies to detect spoofed addresses



Hiveint

Threat Model S.T.R.I.D.E: Tampering

Tampering

- Tampering refers to malicious modification of data or processes. Tampering may occur on data in transit, on data at rest, or on processes.
    - This category is concerned with **integrity**.
- **mHealth Security Perspective**: Attacker modifying data in transit (e.g. from Body Area Networks (BAN) to Local Area Networks (LAN)) or at rest

Mitigations/Countermeasures

- Strong authorization: Appropriate access control mechanisms such as role-based access control (RBAC) must be deployed with least privileges and separation of duties principles. Users must be assigned to access with minimum privileges.
- Data hashing and signing: All confidential data must be hashed and signed to ensure that the data is valid (untampered and came from the correct/expected source).
- Secure communication links: The communication links between system components must be ensured by using protocols that provide message integrity and confidentiality.

Study.com

Threat Model S.T.R.I.D.E: Repudiation

Repudiation

- Repudiation refers to the ability of denying that an action or an event has occurred.
  - This category is concerned with **non-repudiation**.
- **mHealth Security Perspective:** Authorized user performs illegal operations and system cannot trace it, other parties cannot prove this

Mitigation/Countermeasures

- Secure audit trails: All activities (such as successful and unsuccessful authentication) and sensitive data (e.g. cookies and authentication credentials) must be logged and recorded.

Infosec

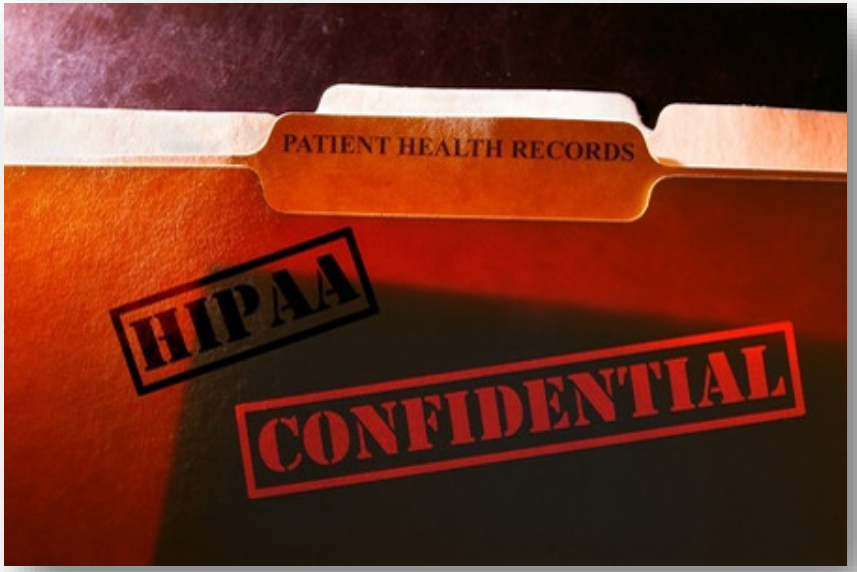
Threat Model S.T.R.I.D.E: Information Disclosure

Information Disclosure

- Information Disclosure refers to data leaks or data breaches. This could occur on data in transit, data at rest, or even to a process.
    - This category is concerned with **confidentiality**.
- **mHealth Security Perspective:** Leaking raw data or medical records

Mitigation/Countermeasures

- Strong authorization: Ensure that an appropriate access control mechanisms is deployed and only authorized users can access to data.
- Encryption: Ensure that all sensitive data is encrypted (in storage or during transit) and only authorized users can read this data.
- Secure communication links: Ensure that all communication links are secured with protocols that provide message confidentiality.

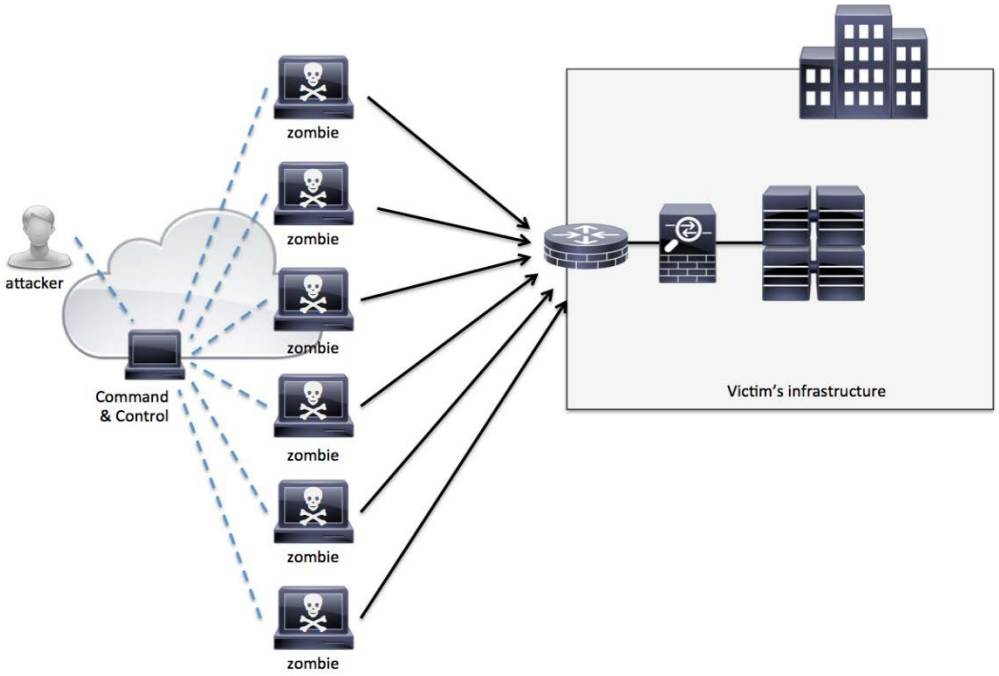


HIPAA Journal

Threat Model S.T.R.I.D.E: Denial of Service

Denial of Service

- Denial of Service refers to causing a service or a network resource to be unavailable to its intended users.
  - This category is concerned with **availability**.
- **mHealth Security Perspective :**Attacker jamming BAN or DoS'ing hospital environment
  - Mitigating this class of security risks is tricky because solutions are highly dependent on a lot of factors.



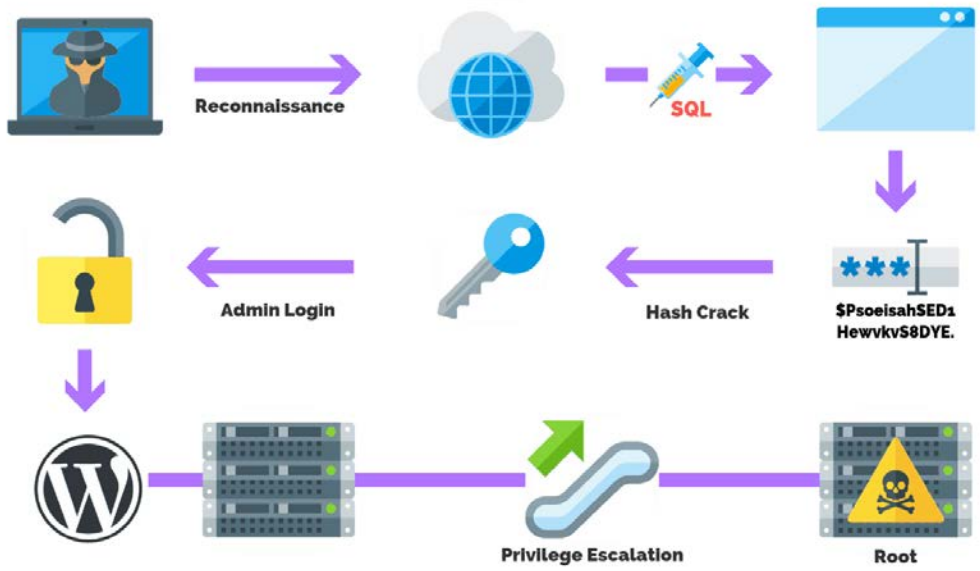
Threat Model S.T.R.I.D.E: Elevation of Privileges

Elevation of Privileges

- Elevation of Privileges refers to gaining access that one should not have.
  - This category is concerned with **authorization**.
- **mHealth Security Perspective :** Attacker gains access to security systems as a trusted entity

Mitigation/Countermeasures:

- Proper authorization mechanism (e.g. role-based access control).
- Principle of least privilege : All authorized user must have a least privilege and minimum required access.



Threat Model Implementation: Authentication Threats

Threat Class 1: Authentication Threats		
Description	STRIDE	Impact
Patient identity loss or identity sharing: the patients leave their login credentials on a public place (e.g. write them down on a piece of paper) or share hem with family, friends or relatives.	Spoofing	Low
Personnel identity loss or identity sharing: healthcare providers, and/or system admins leave their login credentials in public places or share them with others.	Spoofing	High
Identity spoofing: patients reveal login credentials to someone (e.g. social engineering attack).	Spoofing	Low
Identity theft and misuse: informal healthcare assistant (e.g. friends or family members) misuse patient identity to obtain medical services.	Elevation of Privileges	Medium
Identity theft and misuse: system admins misuse patient identity for malicious acts (e.g. curiosity, disclosure, fraud and/or sabotage).	Spoofing	High
Spoofing of source: patient medical devices may be spoofed by attackers, which may lead to incorrect data being delivered to patient communication devices.	Spoofing	High
Spoofing of source: patient communication devices may be spoofed by attackers, which may lead to data being written to the attacker's target instead of the patients communication device.	Spoofing	Medium
Spoofing of source: Personal/Electronic Health Record (PHR/EHR) servers or telehealth service servers may be spoofed by attackers, which may lead to incorrect data being delivered to PHR/EHR servers or telehealth service servers.	Spoofing	High

Department of Information and Communication Technology University

Threat Model Implementation: Authorization Threats

Threat Class 2: Authorization and Access Threats		
Description	STRIDE	Impact
Unauthorized access: unauthorized access to system data using shared (or stolen) passwords.	Elevation of Privileges	High
Unauthorized access: patient intentional or accidental access beyond authorized privileges.	Elevation of Privileges	Low
Unauthorized access: system admins and informal healthcare professionals gain intentional unauthorized access to patient data for malicious acts (e.g. curiosity, disclosure).	Elevation of Privileges	High
Data tampering: patients intentionally or accidentally modify, add and/or delete data because of over-privileges or inapplicable access control of a resource.	Tampering	Medium
Data tampering: formal healthcare professionals and system admins intentionally or accidentally modify, add and/or delete data because of over-privileges or inapplicable access control of a resource.	Tampering	High
Elevation using impersonation: informal healthcare professionals (e.g. friends or family members) may impersonate the patients context in order to gain additional privileges.	Elevation of Privileges	Medium
Elevation using impersonation: formal healthcare professionals or system admins may impersonate the context of other healthcare professionals or system admins in order to gain additional privileges.	Elevation of Privileges	High
Unauthorized access to administration interfaces: malicious users may be able to gain access to configuration management through administration interfaces.	Elevation of Privileges	High

Department of Information and Communication Technology University

Threat Model Implementation: Privacy Threats

Threat Class 3: Privacy Threats		
Description	STRIDE	Impact
Unauthorized disclosure: patients accidentally access some confidential data via malware or file-sharing tools installed on their communication devices.	Information Disclosure	Low
Unauthorized disclosure: formal healthcare professionals and system admins intentionally or accidentally access some confidential data via malware or file-sharing tools installed on their communication devices.	Information Disclosure	High
Lost device: patients losing their communication devices would cause exposure of sensitive data such as login credentials and PHR.	Information Disclosure	Medium
Stolen device: theft of patient communication devices that would cause exposure of sensitive data such as login credentials and PHRs.	Information Disclosure	Medium
Weak access control: improperly protected data stored in patients' communication devices could allow attackers to read information not intended for disclosure.	Information Disclosure	Medium

Department of Information and Communication Technology University

Threat Model Implementation: Audit and Login Threats

Threat Class 4: Auditing and Logging		
Description	STRIDE	Impact
Potential data repudiation: patient denies or claims not receiving, writing or editing data.	Repudiation	Medium
Potential data repudiation: formal healthcare professionals or admins deny or claim not receiving, writing or editing data.	Repudiation	High
Log files tampering: patients, system admins or formal or informal healthcare providers delete or update log files in any way.	Repudiation	High
Insufficient auditing: logging sufficient and appropriate data to handle repudiation claims.	Repudiation	High

Department of Information and Communication Technology University

Reference Materials

References

- Demystifying STRIDE Threat Models
  - https://dev.to/petermbenjamin/demystifying-stride-threat-models-230m
- Threat Modeling: 12 Available Methods
  - https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html
- Uncover Security Design Flaws Using The STRIDE Approach
  - https://web.archive.org/web/20070303103639/http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx
- The STRIDE Threat Model
  - https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878%28v%3dcs.20%29
- Cyber security and resilience for Smart Hospitals
  - https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
- Qualitative Risk Analysis with the DREAD Model
  - https://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/#gref
- MS ISAC Guide to DDoS Attacks
  - https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf
- A Beginners Guide To The STRIDE Security Threat Model
  - https://www.ockam.io/learn/blog/introduction_to_STRIDE_security_model
- Improving Web Application Security: Threats and Countermeasures
  - https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

References

- Security Risk and Threat Models for Health Care Product Development Processes
  - https://core.ac.uk/download/pdf/38131677.pdf
- Is STRIDE Still Relevant for Threat Modeling?
  - https://blog.securityinnovation.com/stride
- Towards dynamic access control for healthcare information systems.
  - https://www.ncbi.nlm.nih.gov/pubmed/18487814
- Role-based access control in healthcare
  - https://www.healthcareitnews.com/blog/role-based-access-control-healthcare
- Threat modeling for mobile health systems
  - https://ieeexplore.ieee.org/document/8369033
- Uncover Security Design Flaws Using The STRIDE Approach
  - https://web.archive.org/web/20070303103639/http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx
- Maintaining Situational Awareness Is Essential with Today's Cyber Threats
  - https://www.ncua.gov/newsroom/ncua-report/2017/maintaining-situational-awareness-essential-todays-cyber-threats
- Threat Modeling of Internet of Things Health Devices
  - https://www.tandfonline.com/doi/abs/10.1080/19361610.2019.1545278?src=recsys&journalCode=wasr20

References

- What is a Threat Vector and Why it's Important to Define
  - https://www.paubox.com/blog/what-is-a-threat-vector/
- Domain Spoofing: How It Works and What You Can Do to Avoid It
  - https://www.paubox.com/blog/domain-spoofing-how-it-works-and-what-you-can-do-to-avoid-it
- A Cisco Guide to Defending Against Distributed Denial of Service Attacks
  - https://tools.cisco.com/security/center/resources/guide_ddos_defense
- Email Spoofing Part 2
  - https://blog.hivint.com/email-spoofing-part-2-9180fa56e82a
- 2,200 Franciscan Health Patients Notified of Unauthorized PHI Access by Employee
  - https://www.hipaajournal.com/2200-franciscan-health-patients-notified-of-unauthorized-phi-access-by-employee/
- A STRIDE-Based Threat Model for Telehealth Systems
  - https://www.researchgate.net/publication/291766457_A_STRIDE-Based_Threat_Model_for_Telehealth_Systems
- Privilege Escalation Attacks: Types, Examples, And Prevention
  - https://purplesec.us/privilege-escalation-attacks/

Questions

Questions

Upcoming Briefs

- Quantitative Risk Management
- Russian Government's Targeting of America's Health Care Sector

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV