LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Electronic Health Record Systems

02/13/2020

Report #: 202002131000

Agenda

- EHR System Overview
- Widespread Adoption
- Certified Health IT Products
- Types of EHR Implementation
- Threats to EHR Systems
- EHR Cloud
- EHR Vulnerability Examples
- EHR System Best Practices
- References
- Conclusion

Slides Key:

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

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

EHR Systems Overview

Protected Health Information (PHI): any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Electronic Health Record (EHR): an electronic version of a patients medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that persons care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.

Electronic Medical Record (EMR): Older term that is still widely used. It has typically come to mean the actual clinical functions of the software such as drug interaction checking, allergy checking, encounter documentation, and more.

EHR System

An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization.

- Usually procured using third-party software suites.

EHR System Functions

- Identify and maintain a patient record
- manage patient demographics
- manage problem lists
- manage medication lists
- manage patient history
- manage clinical documents and notes
- capture external clinical documents
- present care plans, guidelines, and protocols
- manage guidelines, protocols and patient-specific care plans
- generate and record patient-specific instructions

Widespread Adoption

- In 2011, The Centers for Medicare & Medicaid Services (CMS) established the Medicare and Medicaid EHR Incentive Programs, renamed “Promoting Interoperability programs”
  - Encourages clinicians, eligible hospitals, and critical access hospitals (CAHs) to adopt, implement, upgrade (AIU), and demonstrate meaningful use of CEHRT (Certified EHR Technology).
  - Provides incentive payments for certain Medicaid health care providers to adopt and use EHR technology in ways that can positively affect patient care.

Consisted of three stages:

- **Stage 1:** establishes requirements for the electronic capture of clinical data, including providing patients with electronic copies of health information.
- **Stage 2:** focuses on advancing clinical processes and ensuring that the meaningful use of EHRs supported the aims and priorities of the National Quality Strategy.
  - encouraged the use of CEHRT for continuous quality improvement at the point of care and the exchange of information in the most structured format possible.
- **Stage 3 (2017 and beyond):** focuses on using CEHRT to improve health outcomes.
  - Additionally, modified Stage 2 to ease reporting requirements and align with other CMS programs.

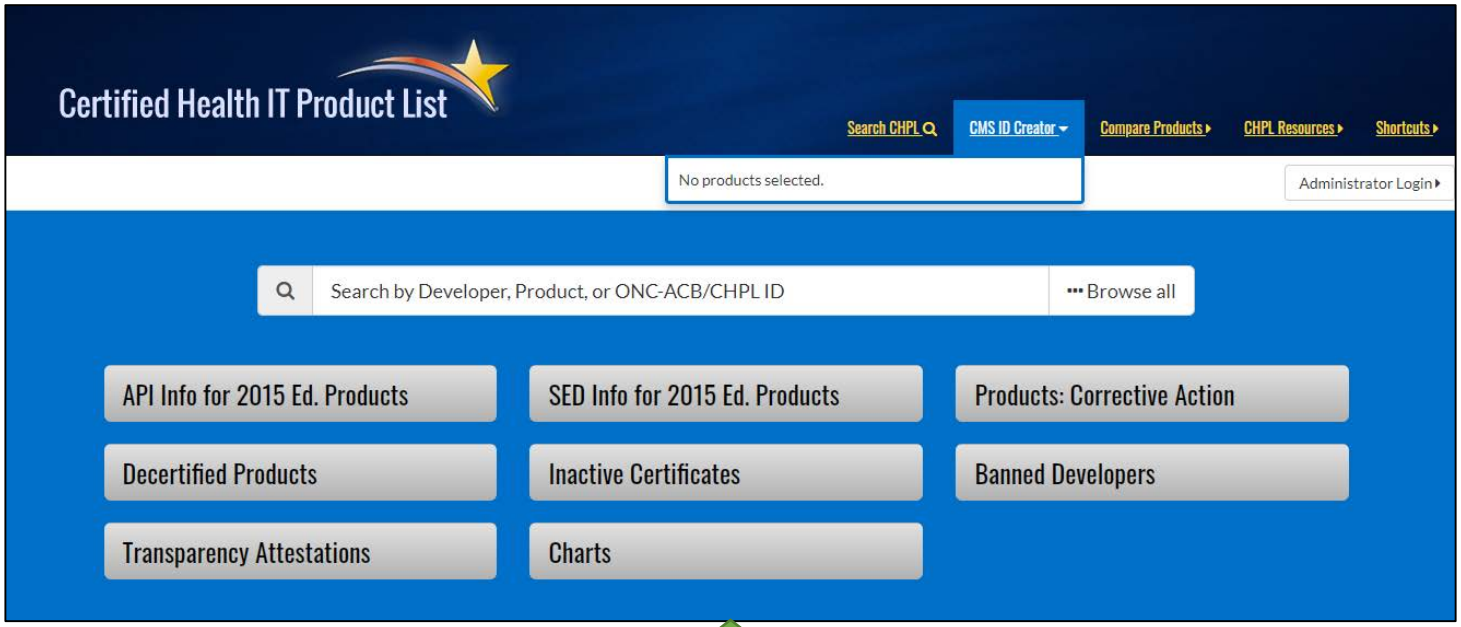
Quick Facts:

- EHR Adoption has more than doubled since 2008
- As of 2017, 86% of office-based physicians had adopted any EHR
  - 80% had adopted a certified EHR

EHR incentive programs have lead to a rapid adoption of EHRs and, thus, a larger enterprise attack surface.

Source: cms.gov

Certified Health IT Products



CHPL Link

The Certified Health IT Product List (CHPL) is a comprehensive and authoritative listing of all certified Health Information Technology which has been successfully tested and certified by the ONC Health IT Certification Program.

All products listed on the CHPL have been tested by an ONC-Authorized Testing Laboratory (ONC-ATL) and certified by an ONC-Authorized Certification Body (ONC-ACB) to meet criteria adopted by the Secretary of the Department of Health and Human Services (HHS).

Source: Healthit.gov

Types of EHR Implementation

Two common types of implementation for EHR systems

Local/in-house
Application deployed on local servers

- Data is kept within the organization
- Can work without an internet connection
- On premises support
- More dependent (software license fees, IT support, maintence, updates)
- Less robust backup

Cloud-based
Third party cloud vendor service
(Often Managed Service Providers)

- Access from many/multiple devices
- Cost effective (typically)
- External backup
- Supply chain threat (data in more places)
- Reliance on third party for support

Increasingly becoming the more common standard

Organizations can also adopt hybrid implementation schemes for more customization

Source: Selecthub

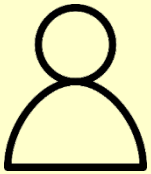
Threats to EHR Systems

Phishing Attacks
Attacker will exploit email, attempting to trick the user into reveling login credentials or installing malicious software onto the EHR system/network.

Malware and Ransomware
Deployed onto a user system in a number ways (phishing, exploits, etc.), malware can impact EHR data; stealing, destroying or holding the data for ransom.

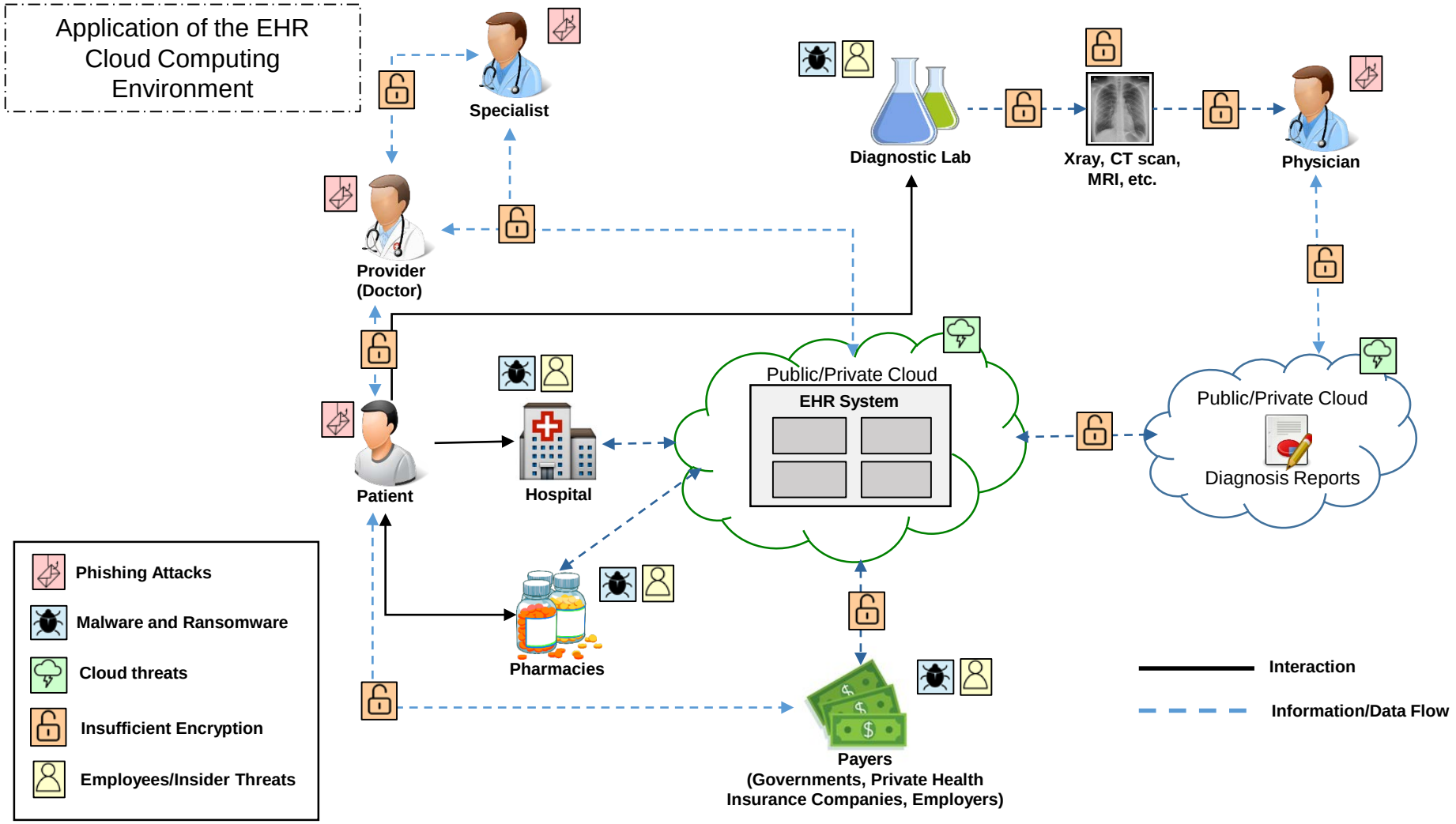
Cloud threats
Cloud services represent a new factor in supply chain/third party exploitation, giving hackers a larger attack surface in which to compromise an EHR system.

Insufficient Encryption
Many devices on the EHR network use little or no encryption, which makes data in transit vulnerable to exploitative attacks, such as Man-in-the-Middle and other exfiltration methods.



Employees/Insider Threats
Personnel within the organization, whether through unwitting negligence or malicious intent, can cause significant damage, using held credentials to gain access to EHR data system.

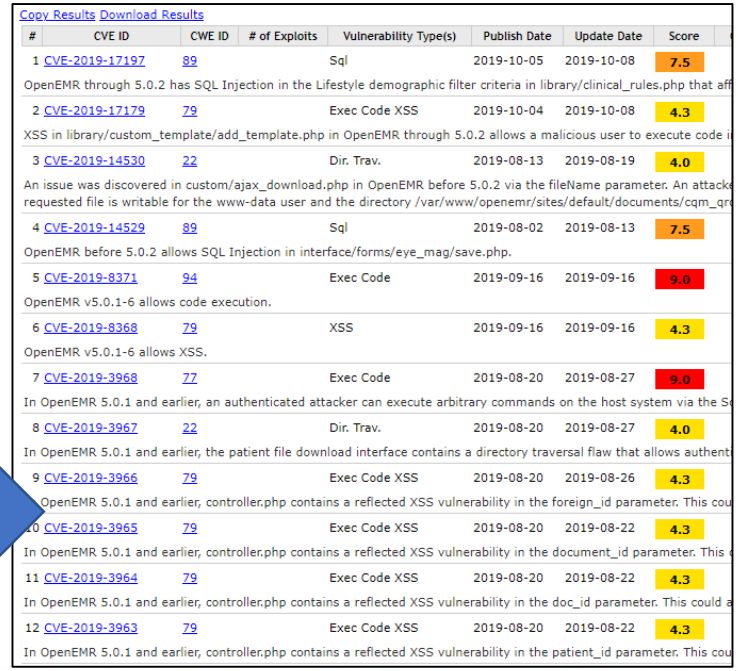
EHR Cloud



Source: Airccse

EHR Vulnerabilities - OpenEMR

- In 2018, OpenEMR a popular open-source EHR platform was found to have more than 20 critical vulnerabilities
  - Nine of the flaws that allowed SQL injection which could be used to view data in a targeted database and perform other database functions
  - Four flaws could be exploited that would allow remote code execution to escalate privileges on the server
  - Several cross-site request forgery vulnerabilities were discovered
  - Three were listed as unauthenticated information disclosure vulnerabilities
- The research was conducted by Project Insecurity, a London-based security firm.
- The vendor was contacted about the flaws and patches were developed to mitigate the issues.
- At the time the report was issued, OpenEMR was estimated to be used by around 5000 healthcare offices in the U.S. and over 15,000 facilities worldwide.
- A quick search shows there have been 12 vulnerabilities associated with the OpenEMR platform in 2019.



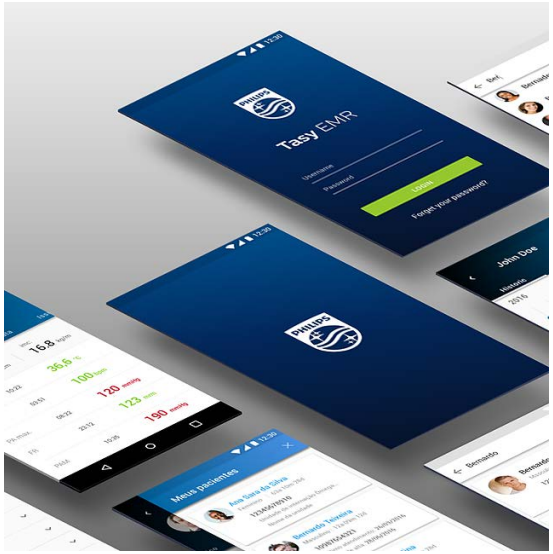
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	CVE-2019-17197	89		Sql	2019-10-05	2019-10-08	7.5
	OpenEMR through 5.0.2 has SQL Injection in the Lifestyle demographic filter criteria in library/clinical_rules.php that aff						
2	CVE-2019-17179	79		Exec Code XSS	2019-10-04	2019-10-08	4.3
	XSS in library/custom_template/add_template.php in OpenEMR through 5.0.2 allows a malicious user to execute code i						
3	CVE-2019-14530	22		Dir. Trav.	2019-08-13	2019-08-19	4.0
	An issue was discovered in custom/ajax_download.php in OpenEMR before 5.0.2 via the fileName parameter. An attacke requested file is writable for the www-data user and the directory /var/www/openemr/sites/default/documents/cqm_qr						
4	CVE-2019-14529	89		Sql	2019-08-02	2019-08-13	7.5
	OpenEMR before 5.0.2 allows SQL Injection in interface/forms/eye_mag/save.php.						
5	CVE-2019-8371	94		Exec Code	2019-09-16	2019-09-16	9.0
	OpenEMR v5.0.1-6 allows code execution.						
6	CVE-2019-8368	79		XSS	2019-09-16	2019-09-16	4.3
	OpenEMR v5.0.1-6 allows XSS.						
7	CVE-2019-3968	77		Exec Code	2019-08-20	2019-08-27	9.0
	In OpenEMR 5.0.1 and earlier, an authenticated attacker can execute arbitrary commands on the host system via the S						
8	CVE-2019-3967	22		Dir. Trav.	2019-08-20	2019-08-27	4.0
	In OpenEMR 5.0.1 and earlier, the patient file download interface contains a directory traversal flaw that allows authent						
9	CVE-2019-3966	79		Exec Code XSS	2019-08-20	2019-08-26	4.3
	OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the foreign_id parameter. This cou						
10	CVE-2019-3965	79		Exec Code XSS	2019-08-20	2019-08-22	4.3
	In OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the document_id parameter. This						
11	CVE-2019-3964	79		Exec Code XSS	2019-08-20	2019-08-22	4.3
	In OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the doc_id parameter. This could a						
12	CVE-2019-3963	79		Exec Code XSS	2019-08-20	2019-08-22	4.3
	In OpenEMR 5.0.1 and earlier, controller.php contains a reflected XSS vulnerability in the patient_id parameter. This cou						

Source: Hipaa Journal

EHR Vulnerabilities - Phillips Tasy EMR

- Two vulnerabilities associated with Philips Tasy EMR were discovered in 2019.
- Philips Tasy EMR advertised as "a comprehensive healthcare informatics solution that touches all areas of the healthcare environment, connecting the dots across clinical and non-clinical domains along the healthcare continuum."
- One vulnerability is a cross-site scripting vulnerability is caused by improper neutralization of user-controllable input during web page generation.
  - The vulnerability requires a low level of skill to exploit by an individual on the customer site or connecting via a VPN.
  - Mostly affects healthcare providers in Brazil and Mexico.
- The EMR also has a information exposure vulnerability which may allow a remote attacker to access system and configuration information
- The vendor has stated: "Philips analysis has shown that it is unlikely that this vulnerability would impact clinical use, due to mitigating controls currently in place. Philips analysis indicates that there is no expectation of patient hazard due to this issue."
- Phillips recommends users update to the most recently released versions of the product.
  - Update Tasy EMR, to version 3.03.1745 or higher and update Tasy WebPortal, to version 3.03.1758 or higher.



Source: Becker Hospital Review, Hipaa Journal, US-CERT

EHR system best practices

- Provide social engineering and phishing training to employees. **[10.S.A], [1.M.D]**
- Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported **[10.S.A], [10.M.A]**
- Ensure emails originating from outside the organization are automatically marked before received **[1.S.A], [1.M.A]**
- Apply applicable patches and updates immediately after testing; Develop and maintain patching program if necessary. **[7.S.A], [7.M.D]**
- Implement Intrusion Detection System (IDS). **[6.S.C], [6.M.C], [6.L.C]**
- Implement spam filters at the email gateways. **[1.S.A], [1.M.A]**
- Block suspicious IP addresses at the firewall. **[6.S.A], [6.M.A], [6.L.E]**
- Implement whitelisting technology on appropriate assets to ensure that only authorized software is allowed to execute. **[2.S.A], [2.M.A], [2.L.E]**
- Implement access control based on the principal of least privilege. **[3.S.A], [3.M.A], [3.L.C]**
- Implement and maintain anti-malware solution. **[2.S.A], [2.M.A], [2.L.D]**
- Conduct system hardening to ensure proper configurations. **[7.S.A], [7.M.D]**
- Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2. **[7.S.A], [7.M.D]**

NOTE: The alphanumeric references listed after each defense/mitigation recommendation are designators for 405(d) Task Group best practices. Background information can be found on page 3 and reference mapping can be found on pages 28 – 30 of the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients located here: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

EHR system best practices continued

Additional Best Practices

NIH NLM

[NCBI Security Techniques for the Electronic Health Records]

[HHS, OCR: Privacy, Security and Electronic Health Records]

Reference Materials

References

- Cloud-based Development of Smart and Connected Data in Healthcare Application
  - http://airccse.org/journal/ijdps/papers/5614ijdps01.pdf
- Understanding Features & Functions of an EHR
  - https://www.aafp.org/practice-management/health-it/product/features-functions.html
- Promoting Interoperability Programs
  - https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms?redirect=/ehrincentiveprograms/
- Cloud-based EHR Systems vs. On-Premise
  - https://www.selecthub.com/medical-software/ehr/cloud-based-ehr-systems/
- Top 5 Cybersecurity Threats to Electronic Health Records and Electronic Medical Records
  - http://integracon.com/top-5-cybersecurity-threats-to-electronic-health-records-and-electronic-medical-records/
- Tennessee hospital's EHR hacked by cryptocurrency mining software
  - https://www.healthcareitnews.com/news/tennessee-hospitals-ehr-hacked-cryptocurrency-mining-software
- EMR vs EHR – What is the Difference?
  - https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference
- More than 20 Serious Vulnerabilities in OpenEMR Platform patched
  - https://www.hipaajournal.com/more-than-20-serious-vulnerabilities-in-openemr-platform-patched/

References

- Vulnerability found in Philips' EMR puts patient data at risk
  - https://www.beckershospitalreview.com/cybersecurity/vulnerability-found-in-philips-emr-puts-patient-data-at-risk.html
- Vulnerability Identified in Philips Tasy EMR
  - https://www.hipaajournal.com/vulnerability-identified-in-philips-tasy-emr/
- ICS Medical Advisory (ICSMA- 19-120-01)
  - https://www.us-cert.gov/ics/advisories/ICSMA-19-120-01
- Security Techniques for the Electronic Health Records
  - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522514/
- Privacy, Security, and Electronic Health Records
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  - https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

- Office-based Physician Electron Health Record Adoption
  - https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php

Questions

Questions

Upcoming Briefs

- PyXie RAT
- NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management

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