CHIME Policy Webinar: Policies Impacting Cyber and Third Party Risk

Sponsored by Fortified Health Security
Today’s Panelists

Mari Savickis
VP Public Policy, CHIME

Dan Dodson
CEO, Fortified Health Security

William Crank
COO, Fortified Health Security
Strengthening the cybersecurity posture of healthcare organizations to protect more patient data and reduce more risk
Healthcare’s Cybersecurity Partner®

Established 2009

100% healthcare focused Managed Security Service Provider (MSSP)

Serving 100+ healthcare organizations

24/7/365 staffed Healthcare Security Operations Center (SOC)

Provides security technology-agnostic services

Leverages client’s existing security technology

INDUSTRY RECOGNIZED
Advisory Services

Developing strategy...
Building security programs...

- Security Risk Assessments (HIPAA, NIST CSF)
- HITRUST Certification
- Virtual Information Security Program (VISP)
- Virtual Information Security Officer (VISO)
- Third Party Risk Management

Healthcare Security Operations Center (SOC)

Monitoring threats...
Guiding remediation...

- Security Information and Event Management (SIEM)
- Connected Medical Device Security Program (IoT/IoMT)
- User Awareness, Education, & Managed Phishing
- Managed Detection and Response (MDR)
- Custom SOC Services

Threat Assessment & Intelligence Services

Identifying vulnerabilities...
Mitigating risk...

- Vulnerability Threat Management (VTM)
- Vulnerability Assessment
- Penetration Testing
- Dark Web Monitoring
- Incident Response
- Threat Indicator Assessment
The New Spring Forum for Digital Health Leaders

Open to all digital health leaders and their teams

Pricing: $395 plus $99 add-on for team members

Special for new registrations only
first 100 new registrations get $100 off Spring Forum or ALL Forum Pass!

See the full agenda and register at chimecentral.org/chime21
Scholarships

• Women & Minority Professional Development Scholarship
• Deadline: April 19
• CHIME Digital Healthcare CIO Boot Camp Scholarships
• Deadline: April 19
• Ignite Education Waivers
• Deadline: May 1
• Federal Policy Landscape Overview
  • Interoperability mandates
  • Privacy nexus
  • Telehealth update
  • Antikick-back / Stark cyber donation
  • Recent court case
  • Foreign Threats
  • Congressional Update

• Moderated discussion
Cyber Risks are Patient Risks

Cybersecurity risks are one of your enterprise risks. These risks can affect every aspect of your organization. The most important risk is **patient safety** which is the cornerstone of every healthcare organization.

Budget, investment, grant funding decisions should consider cybersecurity risk, its impact on enterprise-wide risks and most importantly its impact to patient safety and uninterrupted care delivery.

Common Attack Points for a Healthcare Organization

Networks
Hospital networks without tight access control can let hackers breach one point and move freely within.

Records Disposal
Privacy can be compromised by improper disposal of sensitive information.

Remote Work
Security risks increase with remote Covid-19 testing and vaccination sites, coupled with more nonmedical staff working from home.

Internet of Things
Connected medical devices often lack built-in security features.

Data Storage
Storing electronic medical records, payment and insurance details in a single place increases
Room for Optimism in Oversight

• 2 hard fought winners were secured in past few months:
  • Credit for use of cybersecurity practices now law
  • Cyber donations safe harbor
• MD Anderson court decision
• Increased attention by policymakers
Interoperability Mandates

• **21st Century CURES Act** requirements from 2016 (Section 4004)
  - Interoperability mandates has NOT been delayed
  - CMS payer API rule also not moving forward
  - Spurs significantly more data sharing

• So, what’s the status of information blocking given we are still fighting the pandemic?
  - Administration is focused on vaccine credentialing effort
  - Very little being said about info blocking mandates other than date stands and more FAQs are coming
  - No penalties for providers yet, however, many questions remain
  - Clear that FHIR is seen as pathway forward and APIs are here to stay
Third-Party APIs

- A trove of health data will be released at the request of patients via 3rd party apps putting data into the hands of entities not governed by HIPAA.
- These entities are regulated under a parallel but entirely different universe by the Federal Trade Commission (FTC) which has a very light touch as compared to HIPAA.

- APIs, Privacy, Security Requirements
  - Precious little attention being given to API security
  - According to a recent report of the 30 mobile health apps tested 77% had hardcoded keys they don’t expire and user-names and passwords that were also hard coded
    - Source: https://approov.io
  - Several of these practices run contrary to FTC’s recommendations for app developers
Telehealth Status

- Status of future policies post-pandemic are still in flux
  - PHE extended to April 21
  - HHS promises to extend to end of year
- There are concerns around security with current HIPAA flexibilities
- More telehealth presents more opportunities for cyber incidents
- Plus, more workforce is now at home and many could stay that way
• Per OCR applications that allow for video chats like Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, are permitted to be used by providers without fear of an OCR penalty for non-compliance with HIPAA

• Providers offering telehealth or remote communications technologies may not comply with all HIPAA policies under the pandemic. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

• **Should relaxed HIPAA policies remain post pandemic?**
In a companion set of rules released in late December by the Centers for Medicare & Medicaid Services (CMS) and the Office of the Inspector General (OIG) of last year, the prior administration published new policies that allow for the donation of cybersecurity technology

- New safe harbor
  - Cyber donations now allowed
  - Hardware included; in part

- CMS Rule, CMS Fact Sheet
- OIG Rule, OIG Fact Sheet
Expands definition of technology and services to include hardware primarily used for cybersecurity a key provisions for which CHIME advocated;

Removes the risk assessment requirement originally proposed by the agencies;

Declining to allow the donation of multi-purpose technology unless the primary function is related to cybersecurity;

Declined to permit monetary donations; and

OIG allows any entity to make a donation.
1. Do you plan on taking advantage of the new cyber donation safe harbor?
2. Will you be acting as the donor or donee?
Robocalls

• Congress outlawed it under the **TRACED Act** and it called for FCC to create a Hospital Robocall Protection Group (HRPG)
• CHIME member Dave Summitt of Moffitt Cancer Center was chosen to lead it – was charted for a year
  • Moffitt was targeted with 6,600 calls over 90 days
• They released a set of **best practices** last December
• Multimillion fine **issued** by FCC March 17th – largest ever- while not specific to health it is notable - $225 million fine to Texas telemarketers
Polling Questions - Audience Engagement

1. Has your organization been the victim of robocallers?
2. Has it disrupted patient care?
3. Are your phone carriers willing to work with you to address this issue?
Privacy Intersection

• Large nexus between cyber and privacy including around breaches
• Information Blocking vs HIPAA - oversharing vs under-sharing
  • HIPAA proposed rule still in question – will Biden rule freeze effect it?
• MD Anderson/OCR decision winning court case against OCR
• Vaccine credentialling questions
Breaches involving Third Parties

• One of 2020’s largest breaches involved third parties one involving 550k patients

• Major issues with supply chain exposed during COVID – risk may not be evident until its exposed
  • SolarWinds estimated their incident impacted approximately ≈18k customers

• President just issued an Executive Order on supply chains
Zoom – Remember them?

• Zoom and other platforms have been a critical part of our infrastructure and allow businesses and schools communicate BUT the company was not living up to its promises around privacy and security and FTC took action
  • Mislead consumers about encryption practices
  • Also secretly installed software on mac computers built into Safari browser to bypass protections intended to protect malware.
• FTC will monitor zoom under settlement announced in Nov. 2020 for next 20 years
• Earlier in 2020 FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing
Appetite for Clinical Data is Growing

October 26, 2020 – ripped from the headlines – psychotherapy notes stolen after hack in Finland

Source: Private Psychotherapy Notes Leaked in Major Finnish Hack | SecurityWeek.Com
Foreign Threats

1. Bulletins and recent FBI alerts
2. Serious threats from China, Russia and Iran
Your DNA

• Yup, they are coming for this as well
• More national security concerns

Source: https://www.cbsnews.com/video/us-officials-tell-60-minutes-that-china-is-trying-to-collect-americans-dna/

**APT41** (China)

### Industry targeting timeline and geographic targeting

**Targeted industries:**
- Gaming
- Healthcare
- Pharmaceuticals
- High tech
- Software
- Education
- Telecommunications
- Travel
- Media
- Automotive

**Geographic targeting:**
- France, India, Italy, Japan, Myanmar, the Netherlands, Singapore, South Korea, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, the United States and Hong Kong

Source: HHS’HC3
Congressional Update

• **H.R. 7898** – Requires HHS to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

• $1.9 trillion **American Rescue Plan** includes $650 million for the Department of Homeland Security’s (DHS) Cybersecurity Information Sharing Agency (CISA) though non is directed specifically towards healthcare
Congress Scrutinizes SolarWinds and Microsoft Vulnerabilities

• TBD – Another hearing hosted by Senate Homeland Security and Governmental Affairs Committee (HSGAC)
• April 14 – Senate intelligence open hearing on worldwide threats
• April 15 – House Intelligence also holding worldwide threat hearing
• Mar. 18th - Senate HSGAC on SolarWinds Hacking and cybersecurity Issues
• Senate Intelligence Hearing on SolarWinds Hacking | C-SPAN.org (c-span.org)
• Feb 26th – Joint hearing with House Homeland Security & Oversight and Reform Committees on the Role of Private Tech in the SolarWinds Breach and Ongoing Campaign
• Feb. 23rd - Senate Intelligence Committee on Solar Winds Hacking
• Feb. 10 – House Homeland Security Committee hosts hearing on cyber threats and building resilience
Recent Letters by Lawmakers

• April 6, 2021 – Senate HSGAC requests details on fed response to SolarWinds and Microsoft attacks

• March 17, 2021 – Bipartisan letter from House Energy & Commerce and Oversight and Investigations Committee on SolarWinds to Administration

• May 12, 2020 - Senator Gary Peters (D-MI) letter to President Trump expressing concern over recent Chinese government-initiated attacks of HHS, hospitals and others involved with COVID-19

• April 20, 2020 – Senators Blumenthal (D-CT), Warner (D-VA), Markey (D-MA), Cotton, and Perdue (R-GA) wrote CISA and US Cyber Command about foreign threats targeting healthcare sector
Solarium Report

• What is the Solarium report?
• A report issued in March 2020 by the Cybersecurity Solarium Commission which advocates for a new strategic approach to cybersecurity: layered cyber deterrence.

• 75 recommendations – state deterrence is possible and speed and agility are key

• Commissioners include several lawmakers
  • Senator Angus King (I-ME) – co-chair
  • Rep. Mike Gallagher (R-WI) – co-chair
Are You Plugged into Free Resources??

- **HHS HC3** (aka HHS’ Cyber Command Center)
  - Free Bulletins, webinars, reports.
  - Oh, and they can help if you experience a cyber incident
  - [HC3 Contact Us | HHS.gov](http://HHS.gov)

- **ONC** white paper on API privacy & security considerations

- **Health Sector Coordinating Council**
  - Entire sector welcome – it’s free
  - Great resources, 26 workstreams, listserve

If you suffer a cyber incident and need immediate help from federal authorities & are not getting quick response CALL ME!! We will connect you STAT.
Moderated Discussion
Questions?

Contact Mari at
Mari.Savickis@chimecentral.org
or
reach our entire team at
policy@chimecentral.org