Monthly Cyber Briefing

November 7, 2024

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A chat box.

Materials

Briefing materials and recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Clearwater

Agenda & Speakers

- Cyber Update
- First, Do No Harm: Strategies for Managing AI Risks

Jon Moore

Chief Risk Officer and Head of Consulting Services & Client Success
Clearwater

Dave Bailey

Vice President, Security Services
Clearwater

Clearwater

Cyber Update

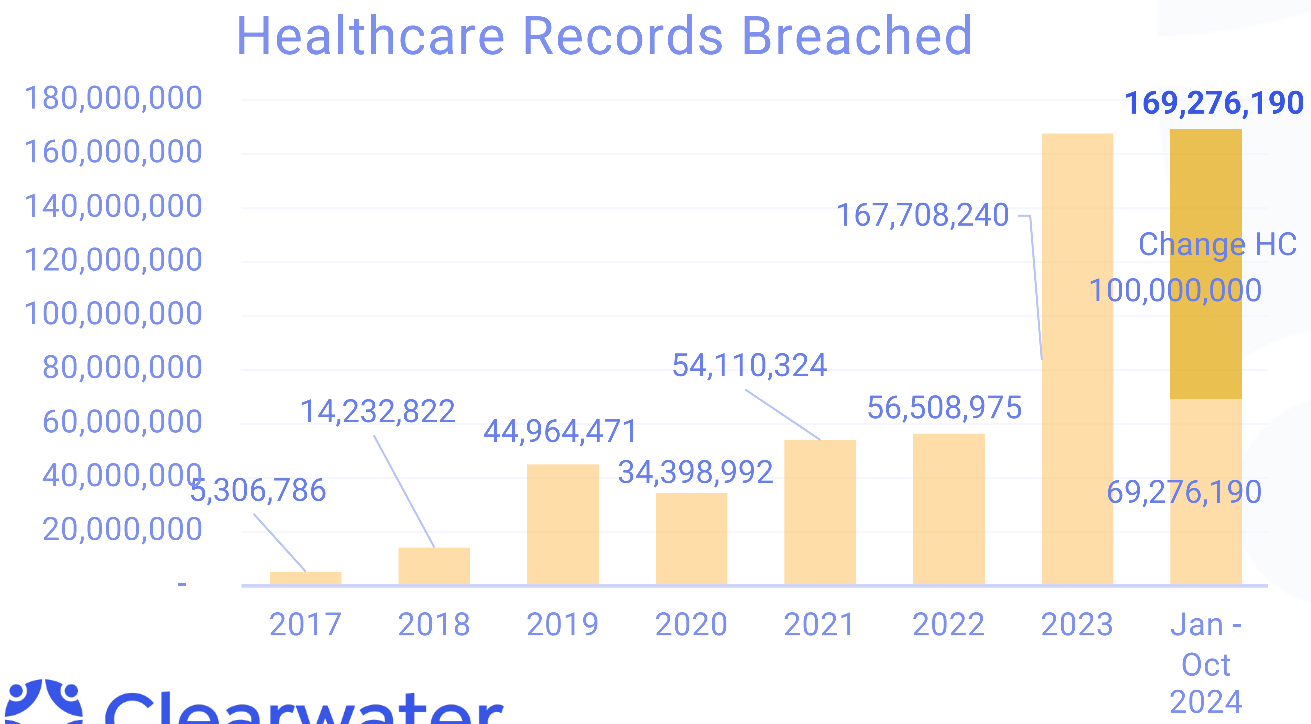
Dave Bailey

Clearwater

Breach Reports via OCR Breach Portal

OCR Breach Portal Data[1]

- In 2023 167.7M records reported as breached vs previously reported 144.4M records reported breached in 2023, an increase of 196% vs 56.5M in 2022
- YTD = 169M records from 581 breaches in 2024; 91% of records due to Hacking/IT Incident

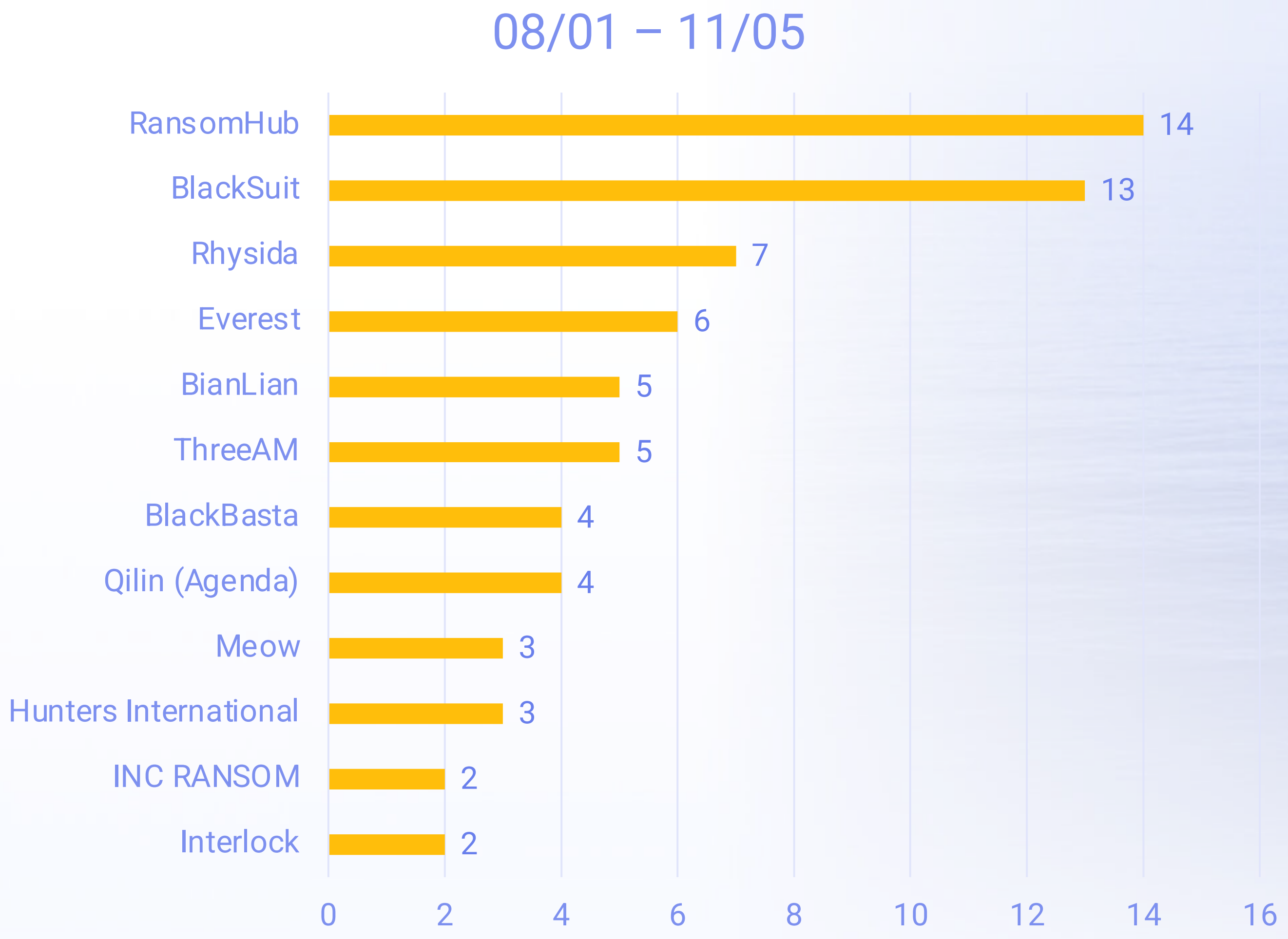


- Number of records breaches in 2023 increased on OCR's Breach Portal by 23.3M records sometime in last few months
- 62 breaches reported since last cyber briefing
- Change Healthcare finally increased number of reported records to 100,000,000
- Largest Breach reported (other than Change Healthcare Care)" Summit Pathology 1.8M records

Clearwater

[1] The HHS Breach Portal (2024 data through 10/31/24, pulled on 11/3/24; 2023 data pulled 11/3/24)

78 US Healthcare victims of ransomware from August to November 5th

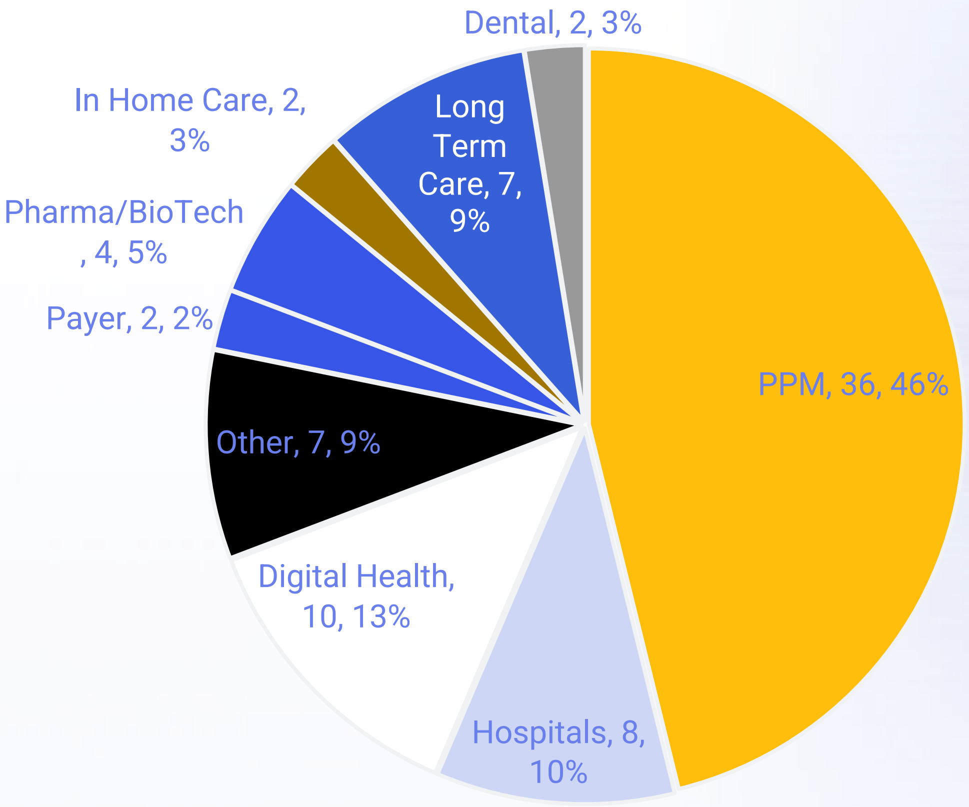


- **RansomHub** & **BlackSuit** attributed with 27 or 35 % of the ransomware attacks during that period
- Ransomware is impacting the entire healthcare sector; These attacks impacted the following segments
  - Physician Practice Management Groups
  - Hospitals
  - Digital Health Companies
  - Long Term Care Facilities
  - In-Home Care Companies
  - Pharma/Bio Tech Companies
  - Payers
  - Dental Organizations

Source: Recorded Future Threat Intelligence

46% of the ransomware attacks from Aug through October were conducted on physician practice management groups

Victim by Industry Segment



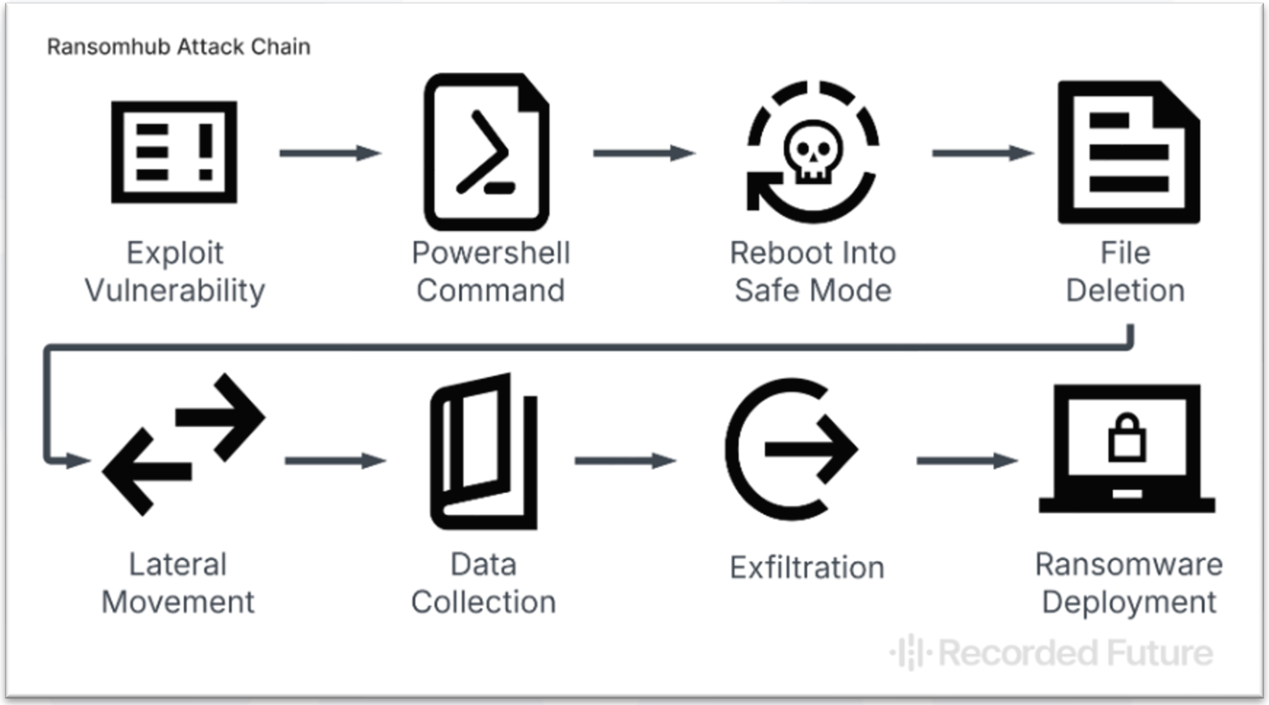
Source: Recorded Future Threat Intelligence

- **RansomHub** , **BlackSuit**, BianLian, & Everst attributed to 64% of the attacks on PPM’s
- The following list of threat actors attacking hospitals from Aug thru Nov 5th
  - Rhysida (CISA Advisory AA23-319A)
  - Embargo (using tools like Mdeployer and MS4Killer for deploying ransomware and disabling endpoint security solutions through vulnerable drivers)
  - Meow (A new resurgence in Healthcare and based on the now disbanded Conti ransomware gang. HC3 Top 10 most active groups in April 2024)
  - Everest (HC3 Threat Actor Profile 202408201700)
  - ThreeAM (Symantec uncovered this ransomware strain after a threat actor’s failed attempt using LockBit in Sep 2023)
  - INC RANSOM (Microsoft Threat Intelligence team recently warned that the Russian speaking Vanilla Tempest ransomware group (previously known as Vice Society) has been actively attacking the healthcare sector.)
  - LockBit (CISA Advisory AA23-165A)

RansomHub offers 90% commission to attract affiliates

As previously reported in August and September, RansomHub has become one of the most active and successful threat actors, building the largest affiliate network.

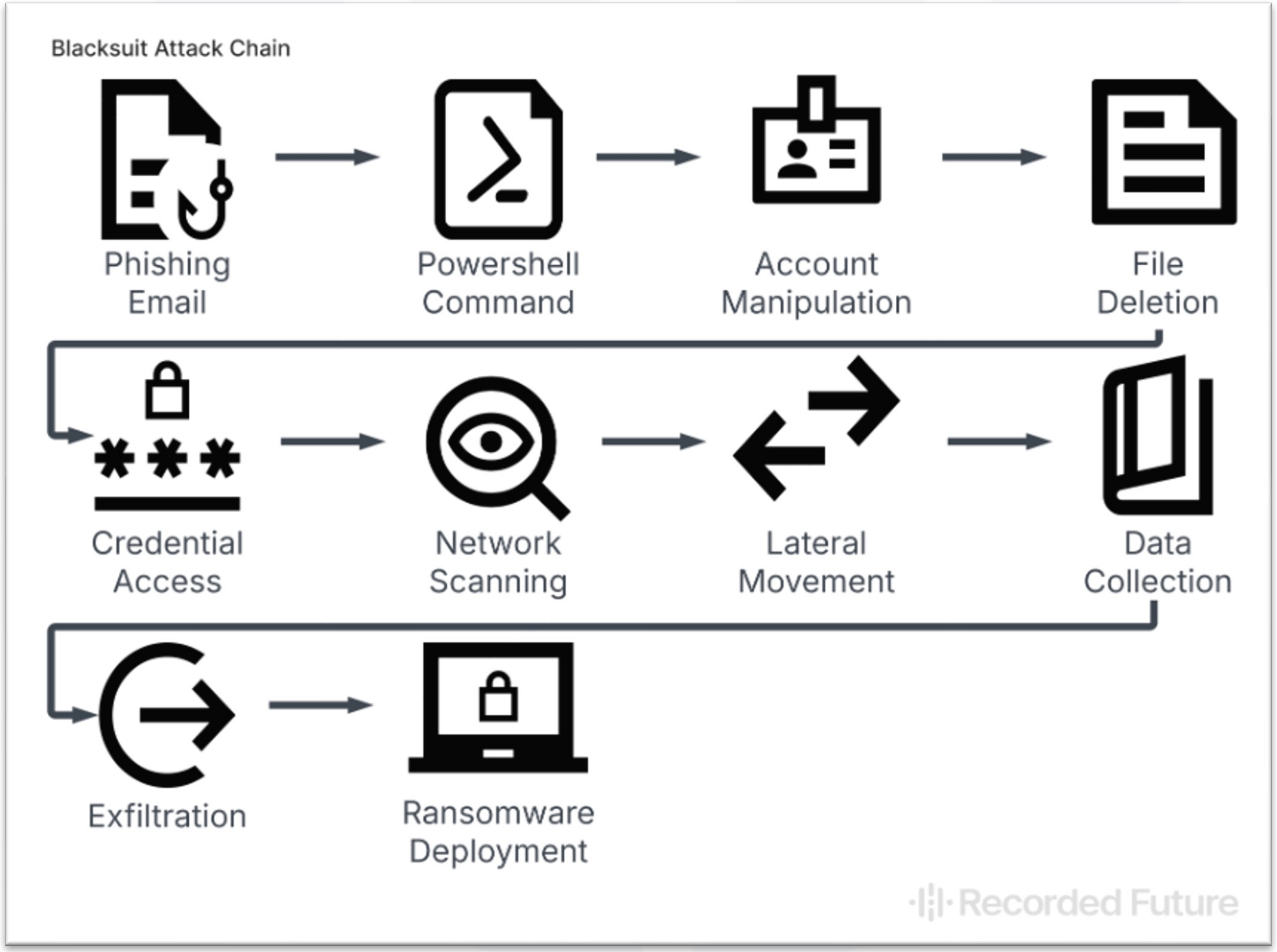
- The FBI and CISA and HHS released a joint advisory to disseminate known RansomHub ransomware IOCs and TTPs on August 29th
- Operates as a Ransomware as a Service (RaaS)
- Gained notoriety in April 2024 when it listed Change Healthcare as a victim on its name-and-shame blog called the "RansomHub Blog"
- Defense evasion techniques include "EDR Killers" such as using TDSSKiller, a legitimate tool from Kaspersky, to attempt disabling endpoint detection and response (EDR) services on target systems, and EDRKillShifter to install drivers with exploitable vulnerabilities



Source: Recorded Future Threat Intelligence

Significant risk posed by BlackSuit due to advanced capabilities and effective use of double extortion

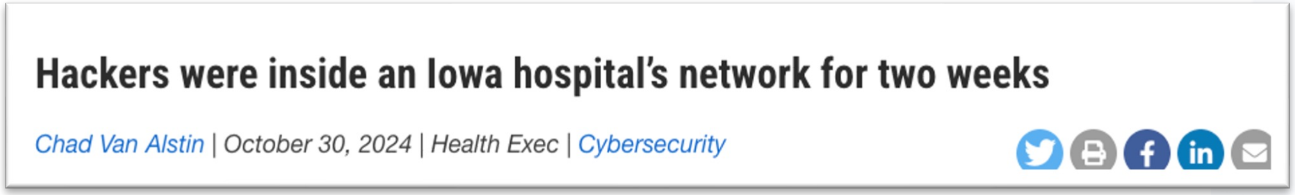
- Joint Cybersecurity Advisory posted on Royal Ransomware Group in Nov 2023
- Advisory updated 3 times during Aug 2024
- They deploy a range of TTPs including Phishing for initial access, exploiting known vulnerabilities such as CVE-2024-4577 and CVE-2020-1472
- Once inside the network it leverages legitimate remote access tools



Source: Recorded Future Threat Intelligence

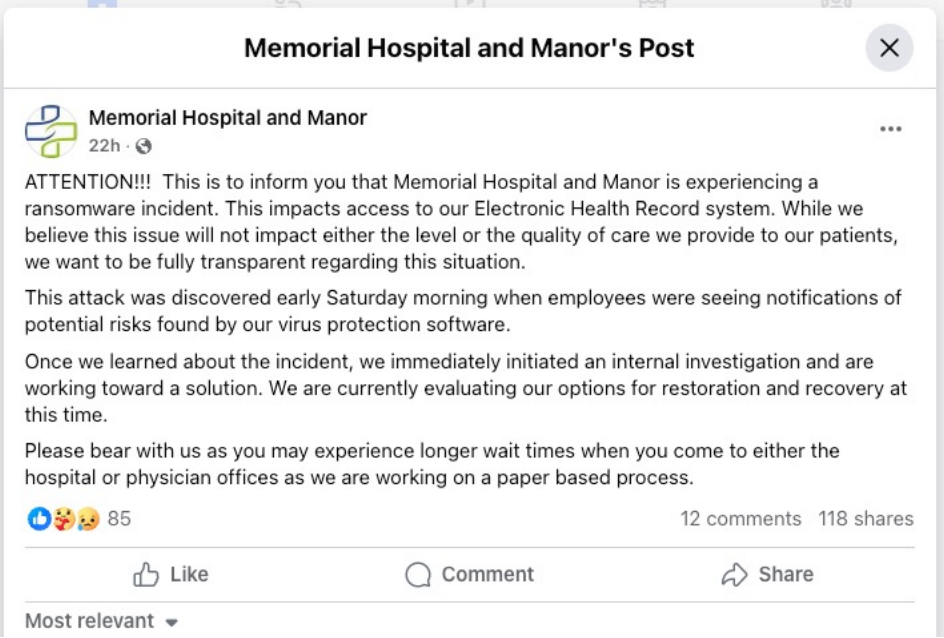
Clearwater

Recent and on-going incidents



Hackers were inside an Iowa hospital's network for two weeks

Chad Van Alstin | *October 30, 2024* | *Health Exec* | *Cybersecurity*



Memorial Hospital and Manor's Post

Memorial Hospital and Manor
22h ·

ATTENTION!!! This is to inform you that Memorial Hospital and Manor is experiencing a ransomware incident. This impacts access to our Electronic Health Record system. While we believe this issue will not impact either the level or the quality of care we provide to our patients, we want to be fully transparent regarding this situation.

This attack was discovered early Saturday morning when employees were seeing notifications of potential risks found by our virus protection software.

Once we learned about the incident, we immediately initiated an internal investigation and are working toward a solution. We are currently evaluating our options for restoration and recovery at this time.

Please bear with us as you may experience longer wait times when you come to either the hospital or physician offices as we are working on a paper based process.

St Anthony Regional Hospital

- Cybercriminals first accessed St Anthony's network on Aug 14 and the breach was not discovered until the 26th
- HHS was notified about the breach on Oct 25 and the impact is not yet determined.

Memorial Hospital and Manor

- On November 3rd Posted on Facebook the organization is experiencing a ransomware incident
- They are currently evaluating options for restoration and recovery
- Notifying the public, they may experience longer wait times coming the hospital or physician offices as they are working a paper-based process

https://healthexec.com/topics/health-it/cybersecurity/hackers-were-inside-iowa-hospitals-network-2-weeks
https://www.beckershospitalreview.com/cybersecurity/georgia-hospitals-ehr-disrupted-by-ransomware-attack.html?utm_medium=email&utm_content=newsletter

Ransomware – Additional Facts and Figures

2,018 Average weekly attacks on healthcare, a 32% increase over last year

$65M Lawsuit settlement for breach of ePHI, including nude photos of cancer patients

$1.3B Estimated cost to Ascension from recent ransomware attack

$2.5B Estimated cost to Change Healthcare from its ransomware attack

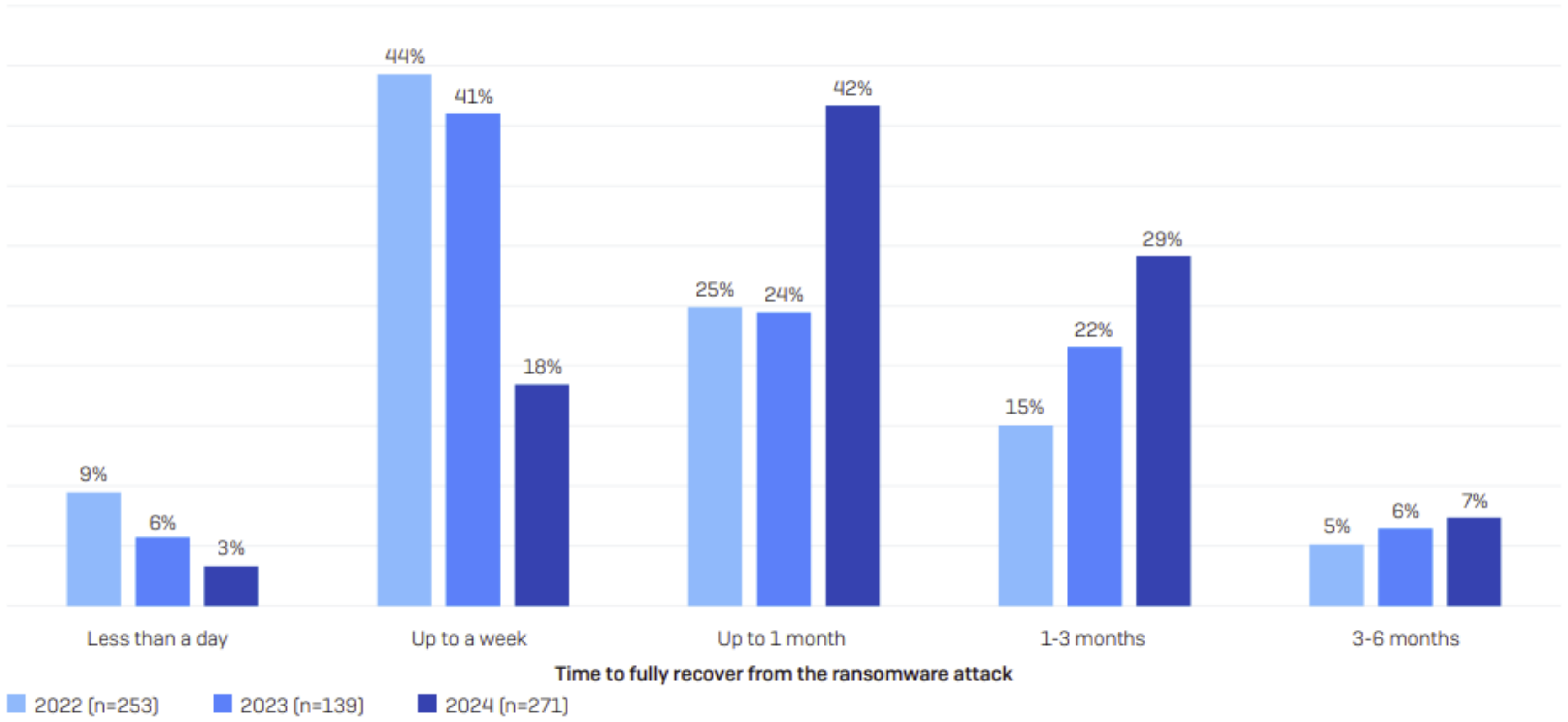
70% Percentage of providers impacted by Change Healthcare ransomware

$1.5M Median ransomware payment of "severe strain" up 650% from 2023

1 Check Point Blog
2 Pa. health system agrees to $65 million settlement after hackers leaked nude photos of cancer patients | CNN Business
3 Ascension financials show $1.3 billion cost from cyberattack | STAT (statnews.com)
4 Change Healthcare's Breach Costs Could Reach $2.5 Billion (bankinfosecurity.com)
5 Healthcare IT Spending: Innovation, Integration, and AI | Bain & Company
6 Ransomware review: September 2024 - ThreatDown by Malwarebytes

Ransomware Recovery Time Increasing

According to a new report by Sophos, the time taken to recover from a ransomware attack has steadily increased in healthcare.



sophos-state-of-ransomware-healthcare-2024.pdf

Numerous APT groups have significantly improved the efficiency of their attacks through AI tools

- The groups are misusing AI for activities like prompt injections, fraud, vulnerability research, scripting tasks, and generating spear-phishing content.
- Reports indicate groups are using AI to automate the development of malware and target specific vulnerabilities more effectively.

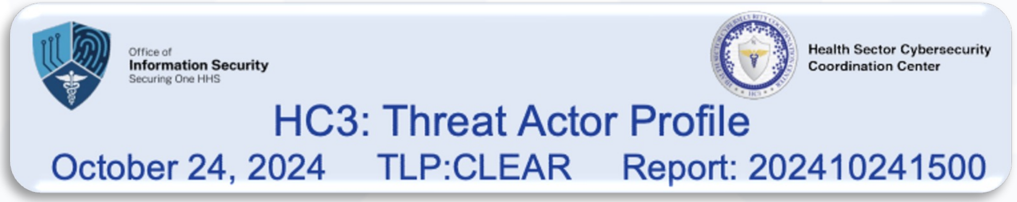
Source: Recorded Future Threat Intelligence

Threat actors leverage AI to launch attacks

OpenAI

Large-scale OpenAI impersonation campaign targeting credentials

- Nov 4th: Threat Actors are sending out phishing emails that appear to come from OpenAI informing recipients their “latest subscription payment for ChatGPT was unsuccessful” and instructing them to clink on a link to update payment information


Office of Information Security Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Threat Actor Profile

October 24, 2024 TLP:CLEAR Report: 202410241500

Feds warn of AI voice spoofing in healthcare

- Oct 24th: HC3 Threat Actor Profile report on Scattered Spider
- The group has become known for its advanced social engineering techniques, including voice phishing and leveraging artificial intelligence (AI) to spoof victims’ voices for obtaining initial access to targeted organizations. The group will likely continue to evolve its TTPs to evade detection.

https://www.securityweek.com/businesses-worldwide-targeted-in-large-scale-chatgpt-phishing-campaign/

https://www.beckershospitalreview.com/cybersecurity/feds-warn-of-ai-voice-spoofing-in-healthcare.html?utm_campaign=bhr&utm_source=website&utm_content=latestarticles

Seven Important Actions Healthcare Organizations Should Take to Address These Threats

1. Know your Adversary
2. Conduct on-going and comprehensive risk analysis; top down to every asset
3. Protect user identities with appropriate authentication
4. Continually train the workforce on current cyber threats and what actions to take
5. Continually test and validate response and recovery plans
6. Patch vulnerabilities
7. Continually validate the effectiveness of your current security controls

First, Do No Harm: Strategies for Managing AI Risks

Jon Moore

Clearwater

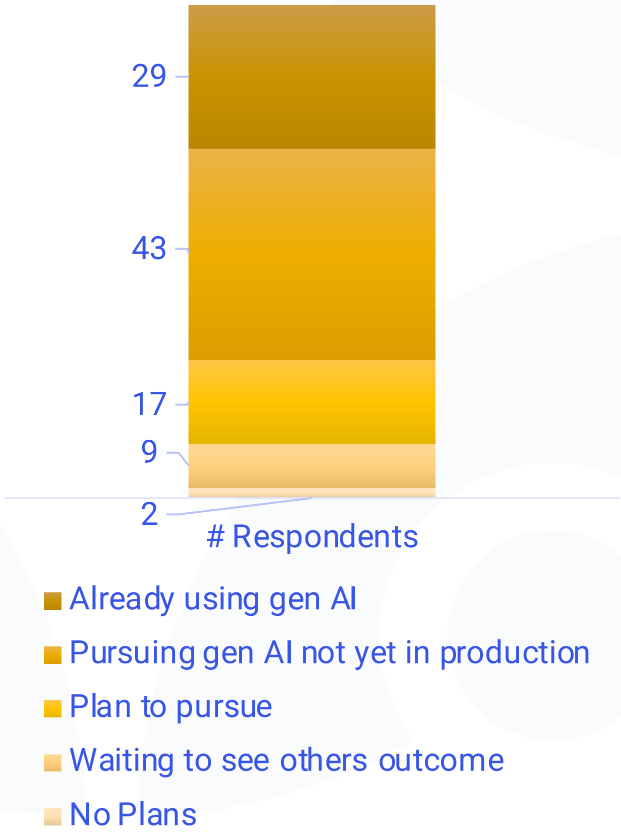
Adoption trends of Generative AI in healthcare

70%

Of respondents from healthcare organizations – including payers, providers, and healthcare services technology groups – say that they are pursing or have already implemented gen AI capabilities

Source: McKinsey US survey on gen AI in healthcare, Mar 11–13, 2024

Healthcare plans to use gen AI



Understanding AI risks

Harm to People

- **Individual**: harm to a person's civil liberties, rights, **physical** or psychological safety, or economic opportunity
- Group/Community: harm to a group such as discrimination against a population sub-group
- Societal: harm to democratic participation or educational access

Harm to an Organization

- Harm to an organization's **business operations**
- Harm to an organization from **security breaches or monetary loss**
- Harm to an organization's **reputation**

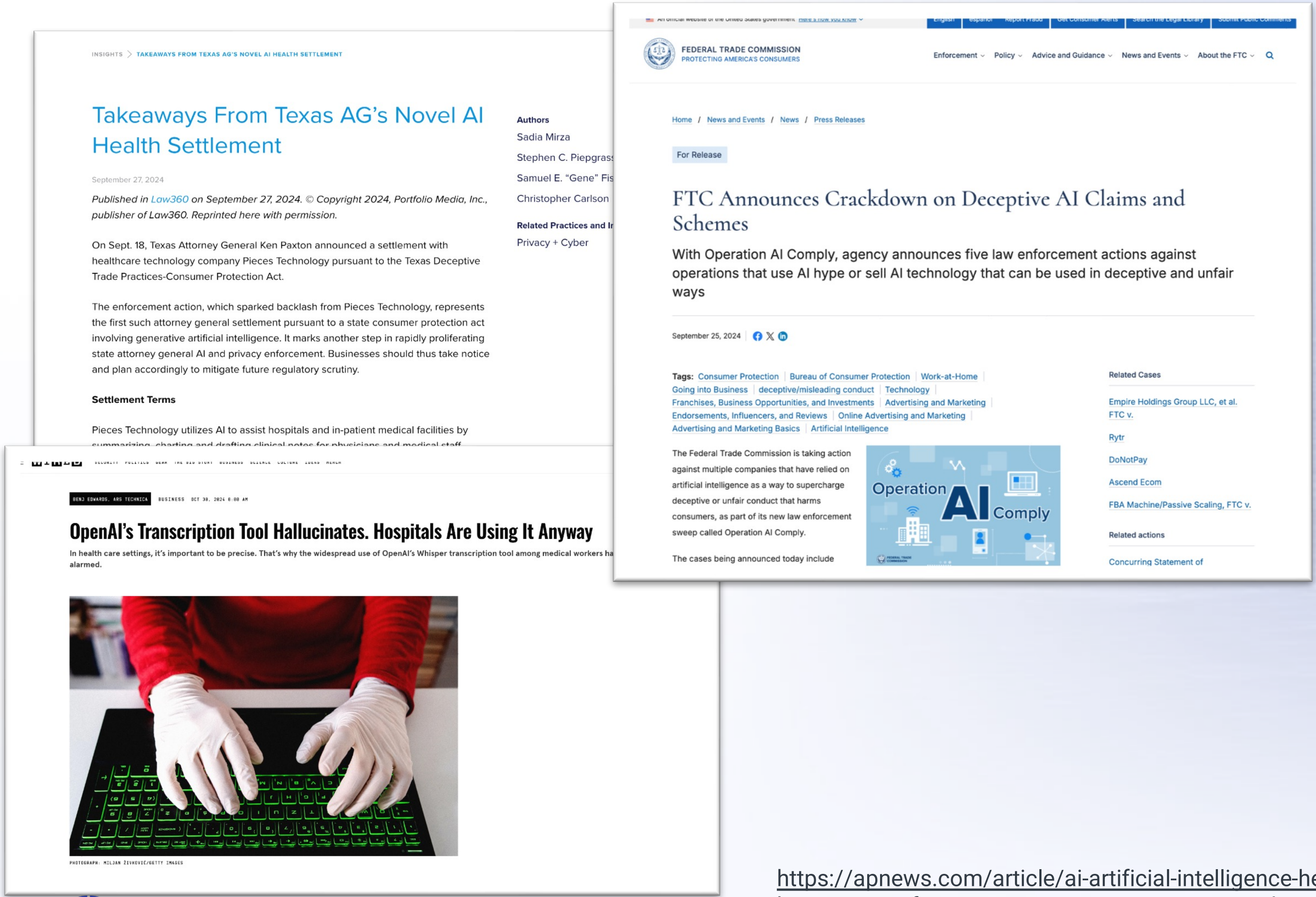
Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources
- Harm to the global financial system, **supply chain**, or interrelated systems
- Harm to natural resources, the environment, and planet

Potential scenarios to understand the impacts of AI failures or misuse

Scenario	Description	Impact
Healthcare Misdiagnosis	An AI system designed to assist in diagnosing medical conditions makes an incorrect diagnosis due to a data bias or algorithmic flaw	• Patients may receive inappropriate treatments, leading to worsening conditions or even fatalities. Trust in AI systems in healthcare could be significantly eroded, delaying the adoption of beneficial technologies
AI Governance and Ethical Violations	The organization deploys AI without proper ethical considerations, leading to violations of privacy, autonomy, or other human rights	• This could result in legal actions, loss of public trust, and calls for stronger AI governance frameworks. The reputation of the organization involved could be severely damaged, and there could be broader societal implications regarding the acceptability of AI
Data Leakage	A cyberattack where a prompt is crafted to manipulate a model into executing unauthorized actions or disclosure of data	• This could lead to breaches of privacy, exposure of proprietary or regulated information, and significant legal and financial consequences for organizations. It could also erode trust in AI systems' ability to safeguard sensitive data

Real Problems Appearing in the Press



INSIGHTS > TAKEAWAYS FROM TEXAS AG'S NOVEL AI HEALTH SETTLEMENT

Takeaways From Texas AG's Novel AI Health Settlement

September 27, 2024

Published in Law360 on September 27, 2024. © Copyright 2024, Portfolio Media, Inc., publisher of Law360. Reprinted here with permission.

On Sept. 18, Texas Attorney General Ken Paxton announced a settlement with healthcare technology company Pieces Technology pursuant to the Texas Deceptive Trade Practices-Consumer Protection Act.

The enforcement action, which sparked backlash from Pieces Technology, represents the first such attorney general settlement pursuant to a state consumer protection act involving generative artificial intelligence. It marks another step in rapidly proliferating state attorney general AI and privacy enforcement. Businesses should thus take notice and plan accordingly to mitigate future regulatory scrutiny.

Settlement Terms

Pieces Technology utilizes AI to assist hospitals and in-patient medical facilities by summarizing, charting and drafting clinical notes for physicians and medical staff

Authors

Sadia Mirza

Stephen C. Piepgrass

Samuel E. "Gene" Fis

Christopher Carlson

Related Practices and I

Privacy + Cyber

An official website of the United States government Here's how you know

English | Español | Report Fraud | Get Consumer Alerts | Search the Legal Library | Submit Public Comments

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement | Policy | Advice and Guidance | News and Events | About the FTC

Home / News and Events / News / Press Releases

For Release

FTC Announces Crackdown on Deceptive AI Claims and Schemes

With Operation AI Comply, agency announces five law enforcement actions against operations that use AI hype or sell AI technology that can be used in deceptive and unfair ways

September 25, 2024

Tags: Consumer Protection | Bureau of Consumer Protection | Work-at-Home | Going into Business | deceptive/misleading conduct | Technology | Franchises, Business Opportunities, and Investments | Advertising and Marketing | Endorsements, Influencers, and Reviews | Online Advertising and Marketing | Advertising and Marketing Basics | Artificial Intelligence

The Federal Trade Commission is taking action against multiple companies that have relied on artificial intelligence as a way to supercharge deceptive or unfair conduct that harms consumers, as part of its new law enforcement sweep called Operation AI Comply.

The cases being announced today include

Related Cases

Empire Holdings Group LLC, et al. FTC v.

Rytr

DoNotPay

Ascend Ecom

FBA Machine/Passive Scaling, FTC v.

Related actions

Concurring Statement of

WIRED SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

BENJ EDWARDS, ARS TECHNICA BUSINESS OCT 30, 2024 6:00 AM

OpenAI's Transcription Tool Hallucinates. Hospitals Are Using It Anyway

In health care settings, it's important to be precise. That's why the widespread use of OpenAI's Whisper transcription tool among medical workers ha alarmed.

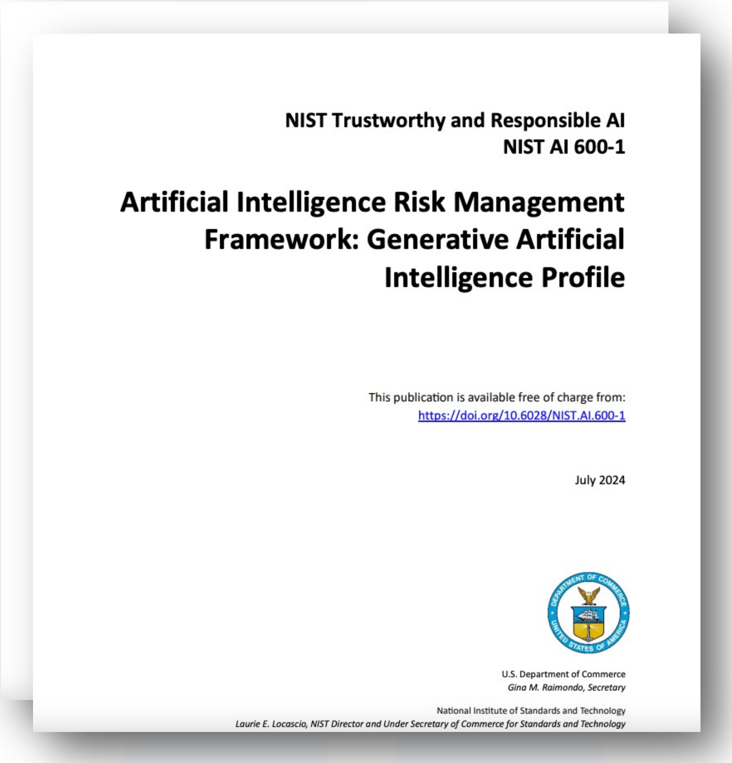
PHOTOGRAPH: MILJAN ŽIVKOVIĆ/GETTY IMAGES

- According to an AP report, over 30,000 medical workers now use Whisper-based tools to transcribe patient visits.
- A University of Michigan researcher told the AP that Whisper created false text in 80 percent of public meeting transcripts examined.
- Another developer, unnamed in the AP report, claimed to have found invented content in almost all of his 26,000 test transcriptions.
- The FTC's investigation found that Pieces Technology made false claims about the accuracy of its GenAI products, including a "severe hallucination rate" of "<0.001%" and "<1 per 100,000."
- FTC announces Operation AI Comply, with five law enforcement actions against operations that use AI hype or sell AI technology that can be used in deceptive and unfair ways

https://apnews.com/article/ai-artificial-intelligence-health-business-90020cdf5fa16c79ca2e5b6c4c9bbb14
https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes
https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-reaches-settlement-first-its-kind-healthcare-generative-ai-investigation

NIST releases Gen AI profile to fulfill the 30 Oct 2023 EO on safe, secure, and trustworthy AI

- Guidance available prior to the release of NIST AI 600-1 did not adequately address AI system risks
  - Harmful bias in AI systems
  - Risks related to generative AI
  - Security concerns related to evasion, model extraction, membership inference, availability, and ML attacks
  - Account for the complex attack surface of AI systems
  - Consider the risks associated with third-party AI technologies, transfer learning, off-label use decision-making outside an organization’s security controls



NIST Trustworthy and Responsible AI
NIST AI 600-1

Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AI.600-1

July 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Adapt your current risk management practices to address generative AI risks

Risk	Description
CBRN Information	Eased access to or synthesis of materially nefarious information or design capabilities related to chemical, biological, radiological, or nuclear (CBRN) weapons or other dangerous materials or agents.
Confabulation	The production of confidently stated but erroneous or false content (known colloquially as “hallucinations” or “fabrications”) by which users may be misled or deceived.
Dangerous, Violent, or Hateful Content	Eased production of and access to violent, inciting, radicalizing, or threatening content as well as recommendations to carry out self-harm or conduct illegal activities. Includes difficulty controlling public exposure to hateful and disparaging or stereotyping content.
Data Privacy	Impacts due to leakage and unauthorized use, disclosure, or de-anonymization of biometric, health, location, or other personally identifiable information or sensitive data
Environmental Impacts	Impacts due to high compute resource utilization in training or operating GAI models, and related outcomes that may adversely impact ecosystems
Harmful Bias or Homogenization	Amplification and exacerbation of historical, societal, and systemic biases
Human-AI Configuration	Arrangements of or interactions between a human and an AI system which can result in the human inappropriately anthropomorphizing GAI systems or experiencing algorithmic aversion, automation bias, over-reliance, or emotional entanglement with GAI systems
Information Integrity	Lowered barrier to entry to generate and support the exchange and consumption of content which may not distinguish fact from opinion or fiction or acknowledge uncertainties, or could be leveraged for large-scale dis- and mis-information campaigns
Information Security	Lowered barriers for offensive cyber capabilities, including via automated discovery and exploitation of vulnerabilities to ease hacking, malware, phishing, offensive cyber operations, or other cyberattacks; increased attack surface for targeted cyberattacks, which may compromise a system’s availability or the confidentiality or integrity of training data, code, or model weights.
Intellectual Property	Eased production or replication of alleged copyrighted, trademarked, or licensed content without authorization (possibly in situations which do not fall under fair use); eased exposure of trade secrets; or plagiarism or illegal replication
Obscene, Degrading, and/or Abusive Content	Eased production of and access to obscene, degrading, and/or abusive imagery which can cause harm, including synthetic child sexual abuse material (CSAM), and nonconsensual intimate images (NCII) of adults.
Value Chain and Component Integration	Non-transparent or untraceable integration of upstream third-party components, including data that has been improperly obtained or not processed and cleaned due to increased automation from GAI

Establish guiding principles for AI acceptable uses

Guiding Principles	Desired Outcomes
Patient Safety	• Patient Safety is always a top priority and any AI application that impacts patient care must adhere to testing and validation as part of risk management
Privacy and Confidentiality	• The use of AI must comply with all relevant privacy laws and hospital policies • Demonstrate AI ethics and responsibility to the use of AI technologies • Build trust with users their data is protected • Ensure permissible disclosures under HIPAA
Transparency	• AI systems must operate transparently, with clear documentation and explainable decision-making processes • Users must understand how AI-driven decisions are made
Bias and Fairness	• AI systems must be designed and tested to minimize biases. • Mechanisms should be in place to recognize bias, error, and other issues • Any identified bias must be documented with corrective measures implemented to ensure fairness in AI-driven decisions
Accountability	• The organization is responsible for the outcomes of AI-driven decisions and ensuring that AI is used correctly, ethically and responsibly

Examples of AI acceptable uses in policy and governance

Acceptable Uses	Desired Outcomes
Clinical Decision Support	• AI may be used to assist healthcare providers in diagnosing and treating patients, provided it is used as a supplement to, and not a replacement for, human judgment.
Operational Efficiency	• AI may be employed to streamline administrative processes, such as scheduling, billing, and resource management, if it enhances the quality of service without compromising patient care.
Research and Innovation	• AI may be utilized in research initiatives aimed at advancing medical knowledge, improving patient outcomes, and fostering innovation, with appropriate ethical oversight.
Patient Engagement	• AI can be used to enhance patient engagement through personalized care, communication tools, and educational resources, provided it respects patient autonomy and consent.

Seven Important Actions Healthcare Organizations Should Take to Manage Cyber Risk While Benefiting from AI

1. Implement Robust AI Governance Program
2. Develop Comprehensive AI Strategy
3. Ensure Compliance with Regulatory Requirements
4. Implement Baseline Cybersecurity Safeguards
5. Conduct Ongoing Risk Management
6. Foster a Culture of Security and Compliance
7. Collaborate with Trusted AI and Cybersecurity Partners

Q&A

Upcoming Industry Events

Fierce Healthcare Payer Summit | Nov 13-14 | Austin, TX

- Steve Cagle is presenting "Tackling Cybersecurity in a Changed Landscape" on Thursday, November 14 from 2:45 PM to 3:30 PM with **Kurt Hagerman**, Field CISO, Oracle, **Darren Lacey**, Former Chief Information Security Officer, Johns Hopkins University and **Christopher Logan**, Vice President & Chief Risk Officer, Blue Cross & Blue Shield of Rhode Island.

- Learn More & Register

Health Sector Coordinating Council
Cybersecurity Working Group

Health Sector Coordinating Council Joint Cybersecurity Working Group All-Hands Meeting | November 19-20, 2024 – San Diego, CA

- Jon Moore, Chief Risk Officer and Head of Consulting Services & Client Success, and Dave Bailey, Vice President of Security Services are attending, and Clearwater is a proud sponsor of the event.

- Learn More & Register

ADSO Next Level Conference | Dec 2 – 4 | Austin, TX

- Don’t miss the opportunity to stop by our sponsor table and engage with industry leaders.
- Dave Bailey, Vice President of Security Services will present 5 Critical Cybersecurity Practices for a Growing DSO at 4:00 pm on December 3.

- Learn More & Book a Meeting With us

Upcoming Webinars

Preparing to Comply with the HIPAA Privacy Rule to Support Reproductive Health Care Privacy | November 14 @ 12:00 CST

- Andrew Mahler and Wes Morris, two leading HIPAA experts and senior leaders of Clearwater's Privacy & Compliance Services team, present an informative webinar to help your organization ensure it is in position to comply with the regulation.

- Register Here

Vulnerability Management Trends: Insights from Clearwater's Security Operations Center | Monthly Cyber Briefing on December 5 @ 12:00 CST

- Steve Akers, Clearwater's Corporate CISO and SOC leader, will discuss key vulnerabilities that healthcare organizations should be monitoring.
- Register Here (Cyber Briefing attendees are already registered)

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.