healthcare dollars & sense.

Selecting the right tool and service providers

This presentation and any oral presentation accompanying it are not intended/should not be taken as necessarily representing the policies, opinion, and/or views of Blue Cross Blue Shield of North Dakota and McKesson/CoverMyMeds, any of their component services, or any other affiliated companies.

This presentation and any oral presentation accompanying it has been prepared in good faith. However, no express or implied warranty is given as to the accuracy or completeness of the information in this presentation.

disclaimer.

about the speakers.

Jay Bobo

Founder, Breachsiren
McKesson + CoverMyMeds

- 20 years in technology
- 10 years in healthcare

Josh Malnourie

Principal Third Party Security Risk Advisor, BCBSND

- Quantifies third party risk
- 18 years in technology
- 15 years in healthcare

goals for today.

1. Review the current regulatory environment and various challenges

2. Facilitate a discussion about the needs of the TPRM community

3. Provide a methodology for selecting the best vendors for your third party risk management program

regulatory overview.

A review of fundamental drivers

regulations.

The aim of mission and regulations is to provide meaningful care while protecting the interests of patients and shareholders by reducing risk.

- HIPAA - PHI
- State laws
- Federal laws
- International laws
- CIRCIA

HIPAA.

Cumulative Selected Enforcement Data (as of Jan 31, 2024)

351,372 complaints

$142,448,772 in fine/settlements

2022 - 55 Million people affected

2074 referrals to DOJ

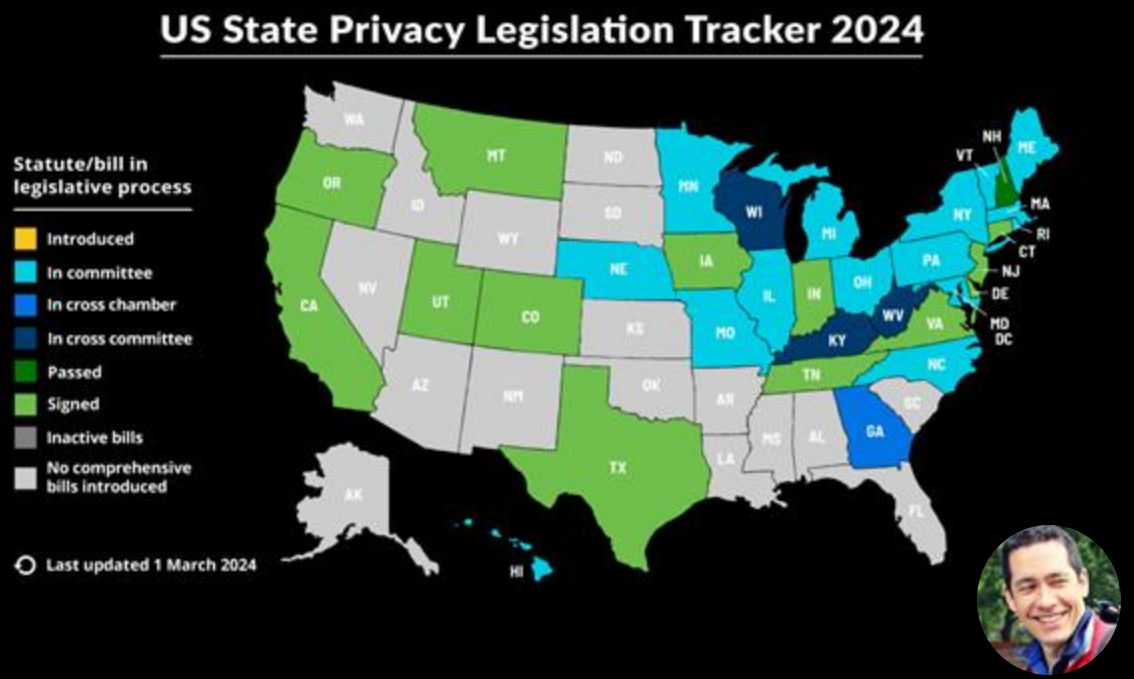
2023 - 134 Million people affected

Selected HHS OCR Recent Settlements/Fines

Company	Date announced	Settlement/Fine	Issue
Montefiore Medical Center	6-Feb-24	$4,750,000	Multiple - insider threat
St. Joseph's Medical Center	20-Nov-23	$80,000	Disclosure of PHI
UnitedHealthcare	31-Oct-23	$80,000	Right of access

state laws.

Make sure your company is tracking latest developments in state privacy legislation - organizations like IAPP can help



international laws.

Make sure your company is tracking latest developments in international privacy legislation - organizations like IAPP can help

CISA rules - CIRCIA.

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022

- Signed in March 2022
- Requires disclosure of breach information and ransomware payment information
- Working on final detailed rules for 2 years
- 447 page notice of proposed rulemaking released March 27, 2024

SEC breach disclosure.

Goal: Reduce financial impact on investors by standardizing disclosures of cyber-related incidents

- Companies must disclose a “cybersecurity incident” on Form 8-K within four business days after determining the incident is material.
- “Not exempting registrants from providing disclosures regarding cybersecurity incidents on third-party systems”
- disclosure may be required by both the service provider and the customer, or by one but not the other, or by neither (materiality)

MeridianLink confirms cyberattack after ransomware gang claims to report company to SEC

Financial software company MeridianLink confirmed that it is dealing with a cyberattack after the hackers behind the incident took extraordinary measures to pressure the company into paying a ransom.

MeridianLink, which reported more than $76 million in revenue last quarter, provides tools to banks, credit unions, mortgage lenders and consumer reporting agencies in the United States.

This week, the company was added to the leak site of AlphV/Black Cat, a ransomware gang believed to be based in Russia that has been involved in several brazen attacks, including the takedown of MGM Resorts.

weaponized disclosure:

Attacker reported MeridianLink to SEC for not disclosing an attack.

Fortunately, attacker reported MeridianLink before the mandatory disclosure came into effect.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

Current Report

Pursuant to Section 13 or 15(d) of

The Securities Exchange Act of 1934

Date of report (Date of earliest event reported): February 21, 2024

UNITEDHEALTH GROUP INCORPORATED

(Exact name of registrant as specified in its charter)

Item 1.05. Material Cybersecurity Incidents.

On February 21, 2024, UnitedHealth Group (the "Company") identified a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems. Immediately upon detection of this outside threat, the Company proactively isolated the impacted systems from other connecting systems in the interest of protecting our partners and patients, to contain, assess and remediate the incident.

The Company is working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate the duration or extent of the disruption at this time. The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies. At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.

During the disruption, certain networks and transactional services may not be accessible. The Company is providing updates on the incident at https://status.changehealthcare.com/incidents/hqpjz25fn3n7. Please access that site for further information.

As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

cybersecurity disclosure:

UnitedHealth notified the SEC on the same day of the Change Healthcare attack.

"As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations".

FTC regulations.

There's two things to know:

1.

FTC Health Breach Notification Rule applies to certain businesses that aren't covered by HIPAA – specifically, vendors of personal health records (PHR), PHR related entities, and third party service providers. (500 records or more)

2.

The FTC Act prohibits companies from engaging in deceptive or unfair acts or practices in or affecting commerce. This means that companies must not mislead consumers about what's happeni with their health information

PRESS RELEASE

Digital Healthcare Platform Ordered to Pay Civil Penalties and Take Corrective Action for Unauthorized Disclosure of Personal Health Information

Wednesday, February 22, 2023

Share

For Immediate Release

Office of Public Affairs

The Department of Justice, together with the Federal Trade Commission (FTC), announced today that the government has resolved allegations that GoodRx Holdings Inc., doing business as GoodRx Gold, GoodRx Care, and Hey Doctor (GoodRx), violated the FTC Act and the FTC's Health Breach Notification Rule. Pursuant to a settlement by the parties, a consent order was entered last Friday by the U.S. District Court for the Northern District of California.

The government's complaint, filed on Feb. 1, alleges that by disclosing millions of users' personal health information to third parties without the users' authorization, consent, or knowledge, GoodRx violated the FTC Act's prohibition on unfair and deceptive trade practices and the FTC's Health Breach Notification Rule. The users' information that was disclosed included personally identifying information, as well as details about medications and sensitive health conditions. GoodRx shared this personal health information despite its repeated assurances that the company would protect users' privacy. For example, GoodRx's public policies stated that the

GoodRx:

Fined for sharing sensitive personal health information for years with advertising companies and platforms in violation of its policies.

Failed to report these unauthorized disclosures as required.

FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies

Letters highlight concerns stemming from use of technologies that may share a user's sensitive health information

July 20, 2023

Tags: Consumer Protection | Bureau of Consumer Protection | Health Privacy and Security | Consumer Privacy | Health Privacy

The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.

"When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."

"Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's website," said Melanie Fontes Rainer, OCR

Related resources

Model Letter: Use of Online Tracking Technologies

For Businesses

Blog: FTC-HHS joint letter gets to the heart of the risks tracking technologies pose to personal health information

Complying with FTC's Health Breach Notification Rule

Health Privacy

Topics

Privacy and Security

Enforcement

pixel tracking:

FTC and HHS sent a joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks of online tracking such as Meta/Facebook pixel and Google Analytics.

question:

Are there other regulations that are important to your organization?

Department of Defense CMMC

challenges.

Obstacles that make TPRM difficult

question:

In tackling regulations, what are challenges you've seen that makes the job of managing third party risk difficult?

common challenges.

Limited resources

- Large volume
- Lack of budget and headcount

Market forces

- Increased competition
- Market agility

Complicated tools

- Lack of transparency
- Limited features
- Expensive pricing

Leadership goals

- Change in risk appetite
- New products and sales opportunities

Difficult vendors

- Poor communication
- Refusal to participate
- Lack of documentation

question:

What's the best way to design my TPRM program to meet the common challenges we listed previously?

solution:

The key is understanding your organizational goals

step 0: understand organizational goals.

Josh's Perspective

For not for profit, covered entities...

- Board mandates for risk mitigation
- Quantification of third party risk
- Risk must tie back to and enable business goals

Jay's Perspective

For business associates & for-profits...

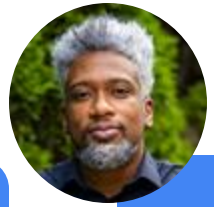
- Commitments to shareholders
- Fulfilling board mandates for risk management (SOC2)
- Enabling growth through innovation and automation (speed)

Does risk tolerance differ based on company size? How?

step 1: research possible vendors.

Josh's Perspective

For not for profit, covered entities...



Jay's Perspective

For business associates & for-profits...

- Know what you need
  - Source transparency
  - How are you going to use what you've paid for?
- Identify options
- Don't get taken by marketing!

step 2: buy or build?

Josh's Perspective

- Cloud first?
- Engage with subject matter experts!

Jay's Perspective

- Vet & build when necessary
- There may not be a solution in the market

step 3: evaluate

Buy Perspective

- Partnership ROI
  - Do they help educate you?
  - Do they only reach out when you submit an incident ticket?
- Communication
  - Are they sharing product roadmaps where they?
  - Do you know when there will be breaking changes?

Build Perspective

Continuous Assessment

- Engage with stakeholders to ensure organizational goals are being met
- Be open to peer & vendor feedback and willing to re-evaluate your creation

the other side.

What should success look like?

What does success look like?

- Patient impact is clear
  - Increased throughput?
- Empathetic third-party risk assessments
  - Vendor morale
  - Team morale
- Clear benefit to peers
- Impact to organizational goals is clear
- There's more ways to get better (evolution)

benefits of having the right tools & vendors.

conclusion.

completed goals for today.

1. Reviewed the current regulatory environment and various challenges

2. Gained an opportunity to learn more about our needs and the needs of others from the TPRM community

3. Obtained methodology for selecting the best vendors for your third party risk management program

things to remember.

1. Focus on organizational goals before developing a TPRM strategy and bringing on vendors

2. View our checklist for questions and best practices to consider when hiring vendors for your third party risk management program

Q&A


"That's all Folks!"