

# Cybersecurity Update

Vendor Interruptions, Best Practices and Preparation

**E×PLORE**  
HEALTHCARE SUMMIT

*The information set forth in this presentation is intended as general risk management information. Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Although reasonable care has been taken in preparing the information set forth in this presentation, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.*



## Today's Topics



### High-Profile Cyber Incidents

Healthcare  
Third-Party Vendors



### Direct v. Indirect Incidents



### How to Prepare Yourself

Education & Best Practices  
Incident Response Planning  
Business Continuity Planning



### When to Notify Insurance





# High-Profile Cyber Incidents

# The Year of Vendor Data & Security Breaches

Third-Party vendor incidents stormed the media in 2024

**BleepingComputer**  
**Integrus Health says data breach impacts 2.4 million patients**  
 Integrus Health has reported to U.S. authorities that the data breach it suffered last November exposed personal information belonging to...  
 Feb 13, 2024



**ABC Chicago**  
**The Lurie Children's outage is having ripple effects across the pediatric medical community**  
 The cybersecurity issue at Lurie Children's Hospital that has spared more than 4,000...  
 Feb 9, 2024



**F** Forbes  
**UnitedHealth Group  
 Cyberattack Costs To Hit  
 \$2.3 Billion This Year**



**NBC News**  
**Outages from Change Healthcare cyberattack causing financial 'mess' for doctors**  
 Change Healthcare's parent company discovered that a cyber threat actor breached part of its network, according to an SEC filing.  
 Mar 1, 2024



**Chicago Sun-Times**  
**800,000 people's data stolen in Lurie Children's Hospital cyberattack**  
 Personal data that was leaked included Social Security numbers, medical conditions or diagnoses, addresses, driver's license numbers and...



## Integris Health

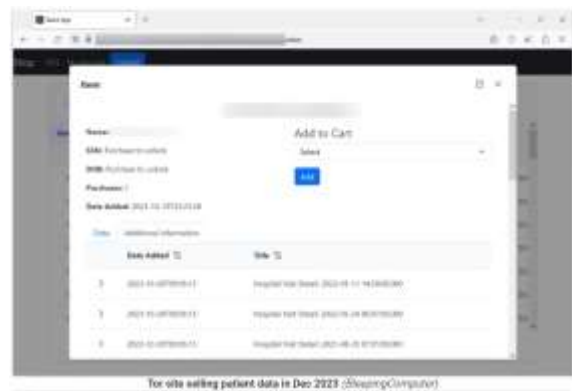
OCR's portal reports 2,385,646 individuals were impacted by the November 2023 Integris Breach

### Threat Actor's Offer:

- \$50 for "removal" of information
- \$3 to view other impacted individual's information

### Impacted Information:

- Full Name
- Date of Birth
- Contact Information
- Demographic Information
- Social Security Number (SSN)



[Integris Health says data breach impacts 2.4 million patients \(BleepingComputer\)](#)

[Integris Health patients get extortion emails after cyberattack \(BleepingComputer\)](#)

## Ann & Robert H. Lurie Children's Hospital

### Rhysida Ransomware disrupts hospital operations and EMR/EHR for partners

- **January 31, 2024:** A cyberattack was discovered and systems were disrupted including EHR and the MyChart patient portal.
- **February 5, 2024:** Systems were partially restored.
- **February 15, 2024:** Email and Phones restored.
- **February 22, 2024:** Lurie Children's continues operations without access to EHR.
- **March 4, 2024:** Lurie Children's electronic health record platform (Epic) was reactivated.
- **March 14, 2024:** Lurie Children's began reactivating their patient portal (MyChart)



## Ann & Robert H. Lurie Children's Hospital

Be prepared to pivot at a moment's notice. Recovery is not a quick flip of a switch.

STATUS UPDATE AS OF 1 p.m. EST, March 14, 2024

Lurie Children's has begun the process of reactivating MyChart for patient families. This process will take place over the coming days.

Currently, key MyChart functions that are coming online to support our patient families include online scheduling, e-check in, provider messaging, and medication refill requests and – in the coming days – bill pay. Additionally, telemedicine appointments will also be available via MyChart. Patient families should refer to their e-mail and/or text message reminders and log into their Lurie Children's MyChart account for information about their upcoming telemedicine appointment.

11/27



Due to the anticipated high volume of MyChart activity, patient families may experience intermittent service disruptions while using the MyChart website/app. MyChart was not updated during the system downtime. We are actively working to update the information available in MyChart with the information collected during the downtime. We do not have an estimate when this work will be complete, and we will provide updates as this process progresses. We thank our patient families for their continued patience.

12/21



Can you go 33 days without access to your Electronic Health Records?





## Change Healthcare

ALPHV/BlackCat Ransomware disrupts one of the worlds largest health payment processing companies

- **February 21, 2024:** Reports from Change Healthcare of a significant network interruption.
- **March 8, 2024:** Restoration of pharmacy services
- **March 15, 2024:** Restoration of electronic payment services
- **March 25, 2024 to April 21, 2024:** Restoration of additional key Change Healthcare products

### The Impact

#### Patients:

- Inability to Process Claims
- Delayed or Denied Care
- Disruption in Pharmacy Services
- Financial Stress and Unexpected Costs
- Potential Data Privacy Concerns

#### Providers:

- Cash Flow Interruptions
- Furloughed Staff
- A Scramble for Loans



What We Learned: Change Healthcare Cyber Attack (House Committee on Energy and Commerce):  
<https://solution-status.optum.com/incidents/hqgjz25fn3n7>

# Change Healthcare

● Uninterrupted / Fully Restored 
 ● Partial Service Available 
 ● Restoration in Progress 
 ● Restoration Date Pending

<p><b>Analytics/Revenue Cycle Analytics</b></p> <p>Analytics provides essential cycle analysis for users of Clearview and Assurance</p> <p>Restored week of <b>4/2/2024</b></p>	<p><b>Assurance/Reimbursement Management</b></p> <p>Batch claim submissions, remittance management</p> <p>Restored week of <b>3/25/2024</b></p>	<p><b>CHC Cardiology PACS</b></p> <p>The on-premise management of images, reports, LOS, biodynamics, workflows, analysis, charge capture, and inventory management.</p>	<p><b>CHC Radiology PACS</b></p> <p>The integrated on-premise web-based PACS system for radiologists.</p>	<p><b>CHC Workflow Intelligence</b></p> <p>The on-premise flexible medical imaging workflow rules engine for radiologists.</p>
<p><b>Clearview Patient Access Suite</b></p> <p>Benefits verification, authorization, financial engagement</p> <p>Restored week of <b>3/25/2024</b></p>	<p><b>Clinical Exchange</b></p> <p>Provider workflow enabling electronic prescribing, ordering and results integrated into LHRs</p> <p>Restored week of <b>4/15/2024</b></p>	<p><b>Compliance Reporter</b></p> <p>Enables NQSA Quality Measure Reporting for HEDIS / CMI Stars, OncITers, Client HEDIS, Chart Abstraction Features</p> <p>Restored week of <b>4/1/2024</b></p>	<p><b>Coverage Integrity</b></p> <p>Coverage discovery</p> <p>Restored week of <b>3/25/2024</b></p> <p>*Modular Workaround</p>	<p><b>Eligibility</b></p> <p>Process real-time transactions</p> <p>Restored <b>4/2/2024</b></p>
<p><b>HealthIQ</b></p> <p>Supports retrospective episode-based payment models</p> <p>Restored week of <b>4/1/2024</b></p>	<p><b>Hosted Payer Services (HPS)</b></p> <p>Payer hosting service for eligibility responses to providers</p> <p>Restored week of <b>3/28/2024</b></p>	<p><b>InterQual Customizer</b></p> <p>Larger plans use this functionality to review and modify the criteria of releases for their own use.</p> <p>Restored week of <b>4/1/2024</b></p>	<p><b>Medical Network Exchange</b></p> <p>For providers submitting HEDIS or CPT codes</p> <p>Claims, enrollment, eligibility transaction processing</p> <p>Restored week of <b>3/25/2024</b></p>	<p><b>MedRX</b></p> <p>Pharmacy electronic claims for medical</p> <p>Restored week of <b>3/25/2024</b></p>



<https://www.unitedhealthgroup.com/changehealthcarecyberresponse>

**Not all large-scale cyber incidents are attacks**



## CrowdStrike Global IT Outage

International Blue Screen of Death (BSOD) day – July 19, 2024



LaGuardia Airport, New York City *(Wikipedia)*



Sydney, Australia *(Stella Qiu, Reuters)*



[https://en.wikipedia.org/wiki/2024\\_CrowdStrike\\_incident#Healthcare](https://en.wikipedia.org/wiki/2024_CrowdStrike_incident#Healthcare)

## CrowdStrike Global IT Outage

### What Happened?

A software update caused millions of Windows users globally to experience the dreaded Blue Screen of Death, leading to system shutdowns, and a "Boot-Loop"

This caused widespread disruption affecting travel, shopping, banking, business operations and so much more.

Concerningly, the disruption impacted Emergency Services, Hospitals, and critical infrastructure.

This was **NOT** an attack. Instead, this was an error attributed for the time being to processes involved in "pushing" updates.

Criminals and other threat groups were equally surprised by this outage. However, they jumped on the opportunities opened.



## CrowdStrike Global IT Outage



**An easy fix in most cases, but a nightmare at scale.**



<https://beazley.security/alerts-advisories/guidance-support-windows-systems-experiencing-boot-loop-due-to-crowdstrike-update>

## CrowdStrike Global IT Outage

### Notable Impacted Health Systems

- Kaiser Permanente
- Providence
- Henry Ford Health
- Nationwide Children's Hospital
- Dana-Farber Cancer Institute
- RWJBarnabas Health
- Emory Healthcare
- Mass General Brigham
- Norton Healthcare
- Penn Medicine
- Seattle Children's Hospital

### The Disruption

- Canceled or Delayed Procedures
- Delayed Cases at Ambulatory Surgery Centers
- Delayed Lab and Pharmacy orders
- Implemented Downtime Procedures for Clinics



[CrowdStrike outage hits US hospitals \(Healthcare Dive\)](#)

[4 Things to know About the CrowdStrike IT Outage's Effect on Healthcare \(MedCity News\)](#)

## CrowdStrike Global IT Outage

### Notable Impacted Health Systems

- Kaiser Permanente
- **Providence**
- Henry Ford Health
- Nationwide Children's Hospital
- Dana-Farber Cancer Institute
- RWJBarnabas Health
- Emory Healthcare
- Mass General Brigham
- Norton Healthcare
- Penn Medicine
- Seattle Children's Hospital

### The Impact

- Approximately 15,000 servers
- Approximately 40,000 of 150,000 devices

### The Response

- Between July 19<sup>th</sup> and July 24<sup>th</sup> Providence leveraged more than 1,000 team members and volunteers to achieve 90% remediation of impacted systems.

**"This is worse than a cyberattack" – Providence CIO, B.J. Moore**



[Hospitals Cancel Nonessential Surgeries After Global Technology Outage \(New York Times\)](#)

[Update: Providence response to CrowdStrike outage \(Providence\)](#)





## Direct v. Indirect Incidents

## Direct v. Indirect Incidents



Retrieved from <https://gastro.org/news/healing-the-healers-understanding-and-addressing-physician-burnout/>

**What control do you have over the resolution of an incident?**





## How to Prepare Yourself

## Education & Best Practices



**You have already  
taken the first step!**



## Best Practices

1. [Establish a Security Culture](#)
2. [Protect Mobile Devices](#)
3. [Maintain Good Computer Habits](#)
4. [Use a Firewall](#)
5. [Install and Maintain Anti-Virus Software](#)
6. [Plan for the Unexpected](#)
7. [Control Access to Protected Health Informaiton](#)
8. [Use Strong Passwords and Change Them Regularly](#)
9. [Limit Network Access](#)
10. [Control Physical Access](#)



## HPH Cybersecurity Performance Goals (CPGs)

HHS partners with CISA to provide support to Healthcare and Public Health (HPH) Critical Infrastructure

### Essential Goals

- Mitigate Known Vulnerabilities
- Email Security
- Multifactor Authentication
- Basic Cybersecurity Training
- Strong Encryption
- Basic Incident Planning and Preparedness
- Unique Credentials
- Separate User and Privileged Accounts
- Vendor/Supplier Cybersecurity Requirements

### Enhanced Goals

- Asset Inventory
- Third Party Vulnerability Disclosure
- Third Party Incident Reporting
- Cybersecurity Training
- Cybersecurity Mitigation
- Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures
- Network Segmentation
- Centralized Log Collection
- Centralized Incident Planning and Preparedness
- Configuration Management

The full CPGs and a [table of CPGs](#) can be found on the [CISA.gov/healthcare](https://www.cisa.gov/healthcare) page



## Incident Response Planning



Who are you going to call?



**Only 63% of Healthcare organizations have a cybersecurity response plan in place**

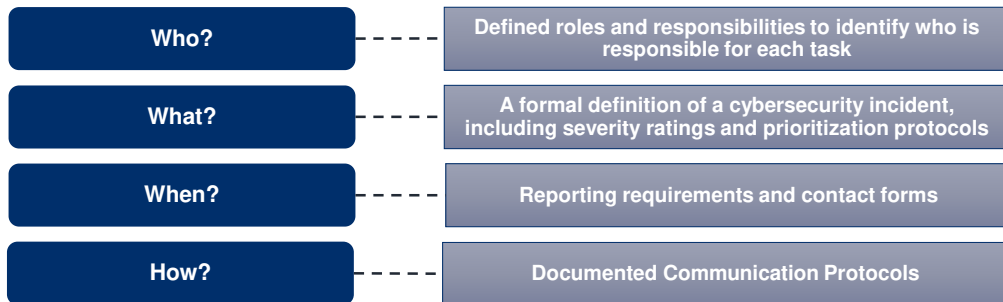
[Software Advice's 2024 Healthcare Data Security Survey](#)





## Incident Response Planning

An incident response plan should ideally include:



## Incident Response Planning

“If you fail to plan, you are planning to fail!”— Benjamin Franklin

### Overlooked Questions:

- Do you have an Incident Response Plan?
  - Where is it?
  - Who is the first person you contact?
    - How do you contact them?
  - What is your involvement in the IRP?
- Do you have Cyber Insurance?
  - Where is your policy?
  - How do you contact your insurer?
  - Do you have a panel requirement?



You do not need to reinvent the wheel when creating an IRP. There are many tried and tested IRP templates.



## Incident Response Planning

Who is on your incident response team?

### The Incident Response Team:

May Include the following departments:

- Legal
- Information Security/Information Technology
- Risk Management
- Communications
- Human Resources
- Privacy Office
- Physical Security
- Business Continuity

May only include:

- Practice Owner
- Practice Manager
- Internal/External IT Manager

Create the team that is right for your organization!



<https://www.softwareadvice.com/resources/healthcare-cybersecurity-threat/>

27

## Business Continuity Planning



How do you keep moving forward during and after a cyber incident?



## Business Continuity Planning

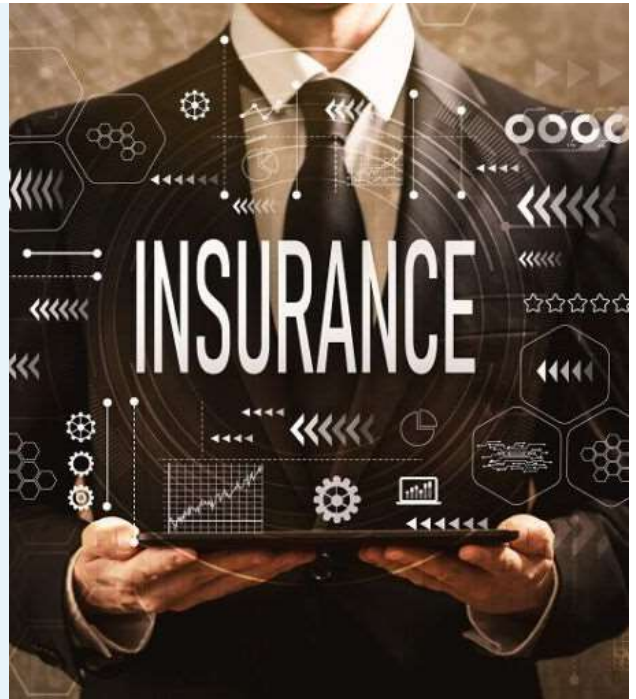
Uninterrupted patient care during and after a cyber incident is crucial

- What is your ability to see patients without an EMR?
- Do you retain paper records or on-prem backups?
- How can you coordinate scheduling?
- What aspects of your practice rely on vendors?
  - Are most systems with one vendor?
- How long can you go without processing claims?
- Do you have easy access to loans or lines of credit?





## When To Notify Insurance



## When To Notify Insurance

- Use your judgement
- Notifying out of an abundance of caution is always better than holding onto a claim
- Running with Incident Response on your own may have negative implications:
  - Often insureds receive bills and then notify insurance
  - Does your policy have a consent requirement?
  - Does your policy have a panel requirement?
  - Did you wipe systems and jeopardize a forensic investigation?
  - Did you over notify?
  - Did you exceed your notification window?

If you see something, say something!



**beazley**



**Tyler Longley**

Beazley Insurance

Assistant Claims Manager – BPS Cyber & Technology

[Tyler.Longley@Beazley.com](mailto:Tyler.Longley@Beazley.com)

