American Hospital Association™

Advancing Health in America

KNOWLEDGE EXCHANGE

Exploring Advanced Data Breach Defense for U.S. Hospitals

Early-warning defense measures to mitigate disruptions to clinical operations

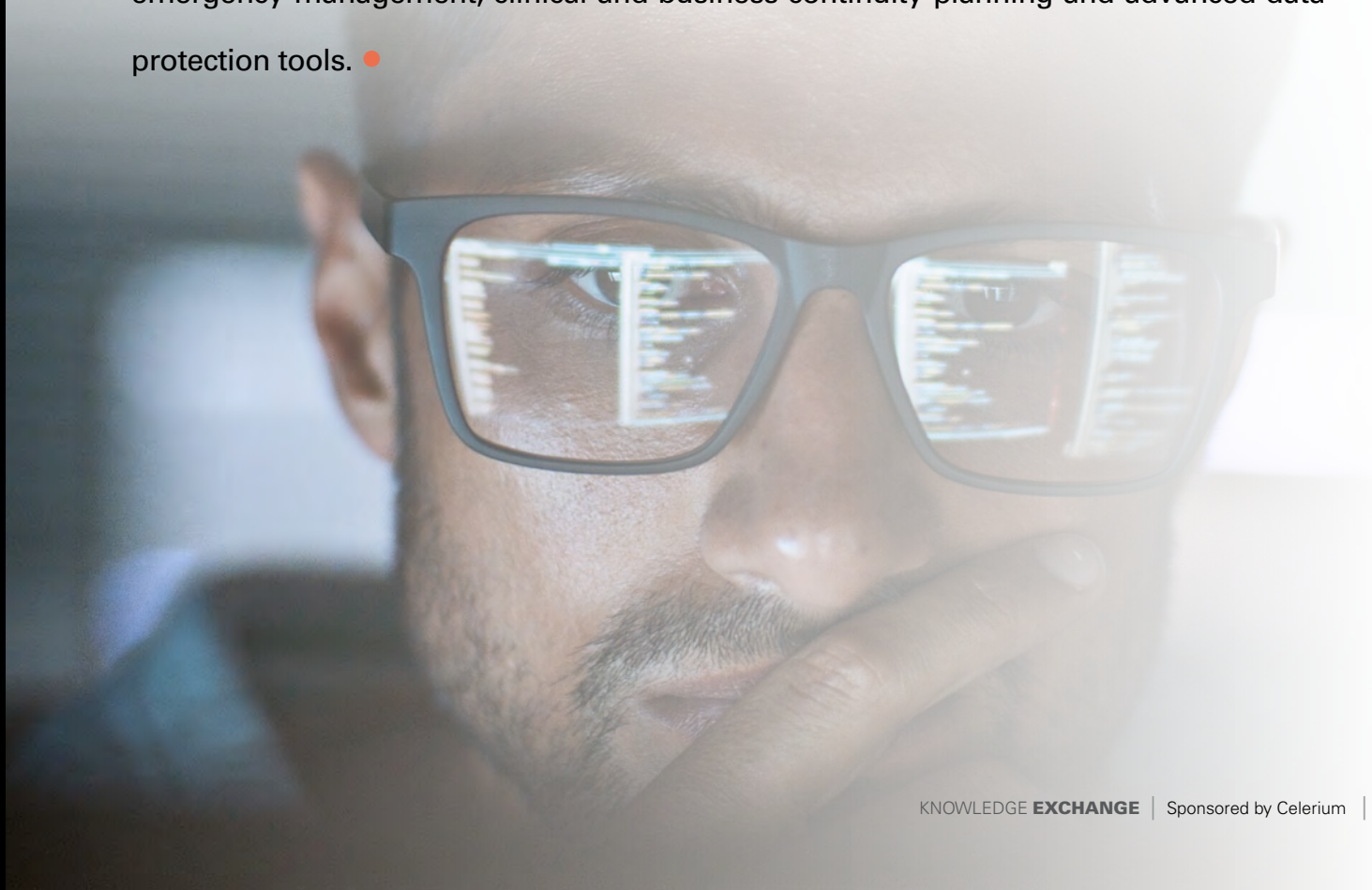
Sponsored by: CELERIUM CYBER DEFENSE SOLUTIONS

Introduction

Exploring Advanced Data Breach Defense for U.S. Hospitals

Early-warning defense measures to mitigate disruptions to clinical operations

Preventing data breaches and containing breaches if they do occur is top of mind for hospital and health system leaders looking to deliver uninterrupted patient care and reduce operational disruptions. Executives and information technology (IT) teams must have clear visibility into breach status at the hospital or clinic level, with leadership tasked with deciding which systems to shut down or isolate. By integrating multiple defensive measures — including minimally invasive containment alongside isolation-based strategies — organizations can strengthen security and reduce clinical disruptions. This Knowledge Exchange e-book explores the importance of early breach detection, emergency management, clinical and business continuity planning and advanced data protection tools.



Action Items

10 proven strategies to prevent and respond to data breaches

1 **Incident command and leadership.** Maintaining a strict chain of command during security incidents is crucial for clear decision-making and response.

2 **Enterprise emergency management.** Physical and cybersecurity, once separate, are now deeply interconnected due to frequent disruptions. Unifying security, emergency management and business continuity strengthens preparedness, response and recovery.

3 **Vulnerability management and security awareness.** Strengthened antivirus protection, identity and access management, and automated patching improve security posture. Additionally, phishing prevention and breach response training remain key priorities.

4 **Emergency preparedness.** Regular drills, tabletop exercises and structured communication ensure effective crisis management.

5 **The role of information technology (IT) in security incidents.** IT should focus on recovery rather than lead the response; dedicated emergency management teams should handle incidents.

6 **Threat monitoring and response.** Early-stage outbound data blocking helps prevent exfiltration before resorting to drastic containment measures.

7 **Cybersecurity as a process.** Security is continuous, requiring ongoing adaptation to emerging threats.

8 **Shadow IT and legacy systems.** Unknown or unmanaged systems pose significant risks, requiring focused monitoring and oversight.

9 **Communication redundancy.** Secondary communication channels, including an off-network paging system and backup email, ensure secure messaging during outages.

10 **Public-private partnerships.** Collaboration with local, state and federal agencies (e.g., Cybersecurity and Infrastructure Security Agency (CISA), FBI) enhances crisis-response capabilities.

Participants

Ron Belfont, MS, CISSP, CHCIO, CDH-E, ITIL
Chief information security officer
Bayhealth Medical Center
Dover, Del.

Brian Brasser, R.N.
Senior vice president, integrations and operations
Corewell Health
Grand Rapids, Mich.

Emy Johnson, MA
Vice president and chief security officer
Allina Health
Minneapolis

Michelle Joy, MHA, FACHE
President and CEO
Carson Tahoe Health
Carson City, Nev.

Karl Kotalik
Chief solutions officer
Celerium
Torrance, Calif.

Thien Lam
Vice president and chief information security officer
BayCare Health System
Clearwater, Fla.

James Matera, D.O., FACOI
Chief medical officer
CentraState Healthcare System
Freehold, N.J.

Gulshan Mehta, MBA, CHCIO, CDH-E
Chief digital and information officer
Blanchard Valley Health System
Findlay, Ohio

Sandra Scott, M.D.
CEO
One Brooklyn Health
Brooklyn, N.Y

Patrick Wilson, CHCIO, CHISL, CISSP, MA
Chief information security officer
Adventist Health
Roseville, Calif.

MODERATOR
Scott Gee
Deputy national advisor for cybersecurity and risk
American Hospital Association
Washington, D.C.

MODERATOR SCOTT GEE *(American Hospital Association):* **Hospital and health system leaders are operating in an environment of elevated data breach risk. How has your cybersecurity strategy evolved over the last year to improve data breach defense and what drove you to make those pivots?**

SANDRA SCOTT *(One Brooklyn Health):* One of the areas of greatest vulnerability is the end user. We expanded the length of our passwords and added additional authentication. The front-line staff who are logging into various systems daily, really felt the pain. The second area is instituting extra procedures to ensure that vendors have the appropriate cybersecurity measures in place.

MODERATOR: Since you mentioned password complexity and rotation, recent thinking from the cybersecurity community is that you're better off with a complex password but not having to rotate it as often. When you implement complex passwords, the first thing people do is write them down and/or save them electronically. A good complex password with multifactor authentication and other security measures is better than rotating it every 30 days — and it reduces staff dissatisfaction.

MICHELLE JOY *(Carson Tahoe Health):* We're an Epic Community Connect site affiliated with a large university system, which requires us to use Cisco Duo for multifactor authentication. Over the past year, we've expanded that authentication beyond Epic — to all our internal systems, including our enterprise risk management and payroll systems. It's been a pain point for our staff, but the Change Healthcare breach raised organizational awareness about the importance of cybersecurity.

We've also invested in upgrading our security information and event management (SIEM) system, which has enhanced our ability to monitor, analyze and correlate security events in real time. As a result of that effort, we've had to expand our team to support this.

MODERATOR: Cybersecurity is best understood as a system of concentric layers, each reinforcing the other. Multifactor authentication plays a crucial role in this framework, adding an extra barrier against unauthorized access. Likewise, data breach detection is another essential component, helping to identify and mitigate potential threats before they cause significant damage.

RON BELFONT *(Bayhealth Medical Center):* We've used both two-factor and multifactor authentication for years. Recently, we expanded password length requirements, with employees using badge access for single sign-on. A password is entered once at the start of a shift, holding for the duration of the shift, while badge access enables seamless login.

All administrative-level accounts have been moved into a Privileged Account Management platform, with checkouts set to a limited time. To enhance security, users must use multifactor authentication upon checking out of a privileged account, which is a new safeguard for us.

To combat rising threat actor calls posing as patients with lost MyChart credentials, we're implementing CLEAR, an airport security platform. CLEAR has partnered with Epic. Confirming identities over the phone is nearly impossible.

We're implementing a password enforcement tool that prevents weak but technically compliant pass-

MICHELLE JOY | CARSON TAHOE HEALTH

"Over the past year, we've expanded multifactor authentication beyond Epic — to all our internal systems, including our enterprise risk management and payroll systems. It's been a pain point for our staff, but the Change Healthcare breach raised organizational awareness about the importance of cybersecurity."

words. It blocks common dictionary words and medical terms. It also checks for breached passwords, alerting users if theirs appears on the dark web.

THIEN LAM *(BayCare Health System):* If a user clicks on a phishing link, they must change their password and complete security training. Repeat offenses are escalated to their respective managers, directors and vice presidents.

More than a year ago, we replaced our antivirus solution with endpoint detection and response (EDR) technology featuring a roll-back function, allowing infected devices to revert to a previous good state. While initial tests were successful, we plan further lab testing across all devices.

Additionally, we enhanced our tabletop exercises by involving clinical staff and simulating a full patient journey — from emergency department registration, surgery, pharmacy and billing — under information technology (IT) system failure conditions. We've refined this process over the past year and a half across all hospitals.

MODERATOR: That's a great way to walk through plans in detail. Discovering a missed step during actual downtime is the worst time to find out.

PATRICK WILSON *(Adventist Health):* End-user training is critical, especially for busy clinicians and knowledge workers frequently targeted by scams. Make the education relevant to their professional and personal lives if possible.

GULSHAN MEHTA *(Blanchard Valley Health System):* We've strengthened antivirus protection, identity and access management, and automated patching for better vulnerability management. While security investments continue, we've prioritized controllable factors like security awareness training, focusing on phishing prevention and breach-response planning.

At my previous organization, we implemented Code Dark, a breach-response protocol ensuring immediate action. Staff carry badge instructions for rapid reaction, similar to a Code Silver (active shooter).

Recent Change Healthcare challenges reinforced the need for realistic contingency planning. While some risks are beyond our control, we're optimizing response strategies while continuing to secure funding for essential tools.

KARL KOTALIK *(Celerium):* Gulshan's point connects to my experience in defense, where nation-state threat actors relentlessly target contractors' intellectual property. Even with robust front-end security — longer passwords, managed detection and response (MDR), EDR — attackers still find ways in, especially given the high value of health care data, now surpassing financial data.

Our focus is on reinforcing back-end security, closely monitoring outbound data flow, particularly sensitive information in systems and backups. Since backups often contain valuable data, attackers may try to exfiltrate them first as part of double extortion — selling stolen data on the dark web if recovery negates ransom payments.

Is there an emphasis on this extra layer of defense — monitoring outbound sensitive data — to stop breaches at the extraction stage rather than just the entry point?

MEHTA: Yes, Karl, I want to know as soon as possible whether it's an attempted breach, an inactive presence or active malicious behavior. Our MDR setup detects anomalous data exfiltration. The real chal-

RON BELFONT | BAY HEALTH MEDICAL CENTER

"To combat rising threat actor calls posing as patients with lost MyChart credentials, we're implementing CLEAR, an airport security platform. CLEAR has partnered with Epic. Confirming identities over the phone is nearly impossible."

lenge is managing data once it has left our network, where we have little control beyond fragile business agreements with legacy vendors. How do we better understand its fate once it's outside our oversight?

MODERATOR: It's not if, it's when, right? How well are you prepared to recover and respond? That shift in perspective moves the focus from accepting that a breach will happen to ensuring that teams are equipped to respond and recover effectively.

BELFONT: About two years ago, we strengthened our security approach by hiring a full-time disaster recovery/business continuity analyst. That role ensures robust plans across departments — including paper backups and a black box for critical data — and also oversees business continuity access computers and reporting.

Previously, recovery was an afterthought — we focused on keeping threats out but realized the gap in response planning. We secured leadership support to invest in this role, significantly improving our preparedness.

BRIAN BRASSER *(Corwell Health):* As part of our overall approach, we're actively planning for a variety of scenarios, including extended system downtime spanning several weeks. We've all experienced electronic health record or network downtime but always had backup access, and the broader infrastructure remained relatively stable. We must be prepared for scenarios where we'll have to function internally with limited to no connectivity and interoperability. Now, 60 teams are updating plans to ensure that they are prepared to continue providing exceptional care and support while we're working on system restoration. Ultimately, all this planning is centered around ensuring that we are able to serve our communities effectively.

MODERATOR: How does your organization handle internal data breach notifications? When incidents occur, how are IT teams, the CEO, chief medical officer, chief nursing officer and vice president of clinical operations informed?

JAMES MATERA *(Central State Healthcare System):* Early notification is crucial, but maintaining a clear chain of command is just as important: everyone must follow the incident commander. Downtime procedures often fall short, with inconsistencies in forms and readiness. Regular drills for the command center ensure that it functions properly during incidents.

During our brief Epic downtime, we held frequent briefings and tracked key system statuses. Preparedness and a structured response make all the difference.

MODERATOR: Unity of command is critical in every incident — making sure there's a clear leader and that everybody knows who that is, with decisions and information flowing through them.

WILSON: Testing during the day is crucial because most downtime experience comes from overnight staff. The IT department plays a vital role but shouldn't run incidents — it should focus on recovery. An enterprise emergency management team should lead, freeing IT to focus on recovery alongside incident responders and forensics teams.

EMY JOHNSON *(Allina Health):* Physical security and cybersecurity used to be separate but are now deeply interconnected due to frequent disruptions. Our program evolved from siloed security, emergency management and business continuity into a unified approach, strengthening preparedness, response and recovery.

KARL KOTALIK | CELERIUM

"Our focus is on reinforcing back-end security, closely monitoring outbound data flow, particularly sensitive information in systems and backups. Since backups often contain valuable data, attackers may try to exfiltrate them first as part of double extortion."

EMY JOHNSON | ALLINA HEALTH

"Physical security and cybersecurity used to be separate but are now deeply interconnected due to frequent disruptions. Our program evolved from siloed security, emergency management and business continuity into a unified approach, strengthening preparedness, response and recovery."

Based in Minneapolis, we faced two major crises beyond COVID-19 — a public safety event and an active violent incident that took the life of one of our care team members, physically injured four others and emotionally injured 28,000. These challenges reinforced the need for an enterprise crisis-management program, emphasizing collaboration, drills and clearly defined roles.

Continuous training ensures adaptability as roles evolve, and strong public-partnerships — including local, state and federal agencies such as the FBI, which offers programs like Domestic Security Alliance Council (DSAC) — are essential to enhancing our operations. Clear information flow is crucial, ensuring that top leaders receive timely, accurate updates rather than broad, indiscriminate communications.

BELFONT: Bayhealth has a standing incident-command center managed by the emergency management team, which is part of our physical security team. On the IT side, we adapted the DEFCON scale (the U.S. military's ranking system for defense condition readiness for a potential attack) into Infocon, a sliding threat-assessment system. Green indicates normal conditions, while blue signals slight elevation. As threats increase, notifications expand. With Infocon, yellow alerts public safety and emergency management teams, triggering broader response efforts.

Our incident response team includes the FBI's local field office and a Cybersecurity and Infrastructure Security Agency (CISA) state representative.

MEHTA: Emergency preparedness should follow established protocols rather than being IT-led, as leadership communication is key. This year, we implemented an off-network, web-paging tool for communication during a full system shutdown, addressing a previous gap. With clinical departments, we defined criticality zones — prioritizing essential systems for rapid activation. Business continuity planning refined our reactivation process, ensuring that vital tools like medication administration take precedence over nonessential functions.

MODERATOR: Cybersecurity is not an end state. It is a process. IT will always introduce new tools — often costly, but invaluable when needed.

WILSON: If you're using cloud-hosted, voice over internet protocol, voice services may be unavailable during an outage, so secondary communication channels are essential.

MODERATOR: Has your organization dealt with data breaches and isolation-based containment? How could minimally invasive containment tools improve your response?

KOTALIK: We're focused on selective outbound data blocking, effective in other industries. While containment becomes difficult once attackers spread, early-stage blocking helps prevent exfiltration before resorting to a kill switch. Our priority is monitoring and restricting outbound data to malicious sites.

Shadow IT is a major risk, as seen in the 2023 MOVEit data breach. Many affected organizations were unaware they were using it and ignored vulnerability warnings. We're addressing gaps by identifying shadow IT and monitoring legacy systems lacking EDR/MDR coverage.

Sponsor

CELERIUM
CYBER DEFENSE SOLUTIONS

Powerful, Automated Early-stage Data Breach Prevention and Containment

Celerium delivers cutting-edge data breach prevention, detection and containment solutions that are not only powerful but also easy to implement and manage with minimal IT resources.

With a proven track record of providing advanced cybersecurity solutions, Celerium has spent the past six years supporting the Department of Defense to safeguard the defense industrial base. We have since expanded these solutions to protect hospitals and the broader health care sector. Our Data Breach Defender™ solution, powered by an advanced Decision Engine hosted on the secure AWS cloud, enables health care organizations to rapidly detect and contain potential data breach incidents, significantly reducing both the cost and impact of such threats.

For more information, please visit:

Celerium.com

www.celerium.com/who-we-help/health-care