HHS 405(d)
Aligning Health Care
Industry Security Approaches

# The 405(d) Post

## Volume XX

A Word from the Task Group

# How to Grow Your Security Program Without Busting Your Budget

By Kate Pierce, 405(d) Task Group member

Hospitals across the nation teeter on the brink of closure as they grapple with a challenging combination of historically thin margins, escalating costs, and persistent labor shortages.

Rural hospitals, in particular, face additional challenges related to patient volumes and difficulty recruiting and retaining qualified staff. According to the Center for Healthcare Quality & Payment Reform, approximately 30% of rural hospitals (646 in total) are at risk of closure due to financial burdens.

A correlated report indicates that 1,129 hospitals have experienced persistent financial losses over multiple years, excluding 2020. Unfortunately, as a result, rural hospitals are compelled to reduce services, exacerbating the plight of patients in already underserved regions.

Hospitals are falling behind other industries when it comes to allocating funds for security measures, with only 5% of their budget dedicated to security compared to the industry average of 16%. Unfortunately, the current budget constraints have made it incredibly challenging to increase or even maintain the allocation for safeguarding hospital facilities. In fact, the allocation of IT budget to security has remained relatively stagnant since the 2018 HIMSS Cybersecurity survey.

Furthermore, the United States is grappling with a severe shortage of qualified cybersecurity professionals, which has continued to worsen in 2022. The 2022 HIMSS Cybersecurity Survey reports that a staggering 84% of healthcare organizations encountered difficulties in recruiting skilled cybersecurity personnel, and an additional 67% expressed significant challenges in retaining their existing staff in this field.

Exacerbating these issues is the alarming rise in ransomware attacks targeting healthcare organizations, with data breaches doubling in just three years. Moreover, the cost of recovery from such attacks has skyrocketed to over $10.1 million per incident in 2022.

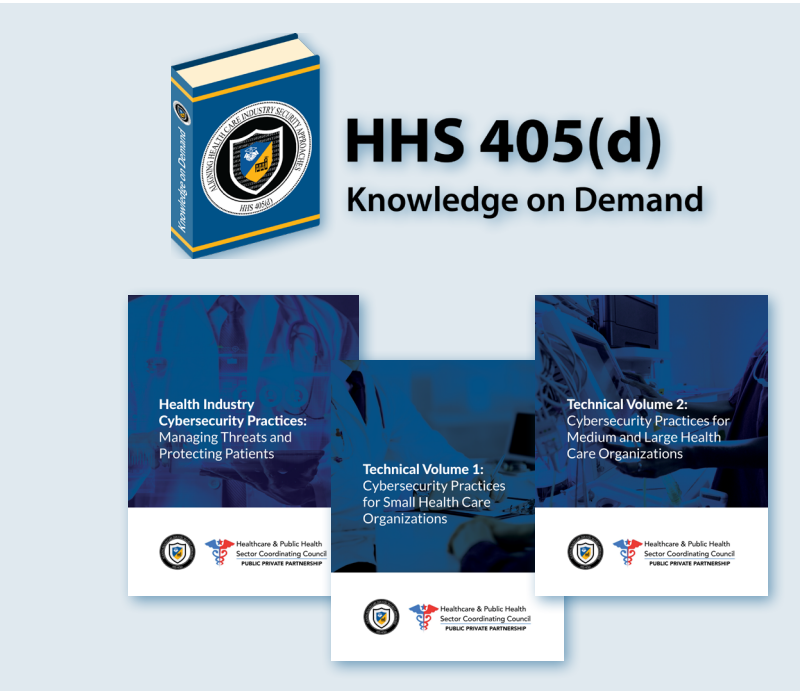
Despite this perfect storm of challenges facing healthcare organizations, there are strategies to enhance cybersecurity programs without incurring exorbitant costs. A wealth of free guidance materials and services provided by the government can be tapped into, offering valuable resources to help hospitals fortify defenses without straining budgets.

In addition to an abundance of free guidance and resources, federal funding specifically designed for emergency preparedness and rural connectivity are available, as are various state and local grants and free programs catering to hospitals of all sizes. These opportunities empower healthcare institutions to fortify their technological assets and enhance their overall security posture.

## Free Resources

The websites below contain a wealth of good (and free!) resources that you can use to improve your cybersecurity posture or find funding opportunities.

**405(d) Program Website** features a plethora of resources including access to the latest industry tested best practices as noted in the Health Industry Cybersecurity Practices (HICP) 2023 Edition. This website also offers a brand-new training platform called Knowledge on Demand that offers free end-user awareness training for the top five cyber threats facing the healthcare industry. There is also a searchable database of free resources, including infographics, newsletters like this one, webinars with slides, awareness posters and more!




**Health Sector Coordinating Council Cyber Working Group** (HSCC CWG) provides resources including a cybersecurity framework implementation guide, video training for clinicians, managing legacy technology security, and artificial intelligence and machine learning.

**Cybersecurity and Infrastructure Security Agency** (CISA) has compiled free cybersecurity tools and services to help organizations advance their security capabilities.

**Administration for Strategic Preparedness and Response** (ASPR) features video, documents, and more to help protect against, mitigate, respond to, and recover from cyber threats.

**National Institute of Standards and Technology** (NIST) Small Business Cybersecurity Corner (SBCC).

## Federal and State Grants and Subsidies

For more than two decades, I served as CIO and CISO for a critical access hospital. We explored many of the grants outlined below and were fortunate to win several that helped us to improve and protect our technology infrastructure. Applying for grants takes time and discipline, but funding programs like these allowed us to maximize our cybersecurity spending.

Please also note that each state has its own Homeland Security Grant program. To identify the program in your state, just a quick internet search is all you need to get details on all FEMA grants.

**FEMA - Nonprofit Security Grant Program** (NSGP): This grant provides funding support for target hardening and other physical security enhancements and activities at 501(c)(3) organizations considered critical infrastructure. Grant money can be used for both physical infrastructure and security software and services. Maximum $150,000 per site for no more than three sites.

**FEMA - State Homeland Security Program** (SHSP): This Homeland Security Grant offers risk-based funds to bolster state, local, tribal, and territorial efforts to prevent, mitigate, respond to and recover from acts of terrorism and other threats. State and municipal hospitals can partner with a state agency through a memorandum of understanding (MOU).

**FEMA - State and Local Cybersecurity Grant Program** (SLCGP): Also appropriate for state and municipal hospitals, these grants specifically address cybersecurity risks and cybersecurity threats to information systems.

**USAC Healthcare Connect Fund (HCF) Program**: This is a subsidy program that provides up to a 65% discount on internet/telecom monthly recurring costs, including equipment and network management services that can include cybersecurity. Consortiums of urban and rural hospitals are eligible if at least 50% of the participants are rural.

**Health Resources & Services Administration** (HRSA): The organization has given more than 3,000 grants to help provide equitable healthcare to disadvantaged groups and the geographically isolated, including telehealth.

USDA Distance Learning and Telemedicine Grants (RUS DLT): Aimed at rural populations of fewer than 20,000 people, grants require a 15% match and provide up to $1 million for distance learning and telemedicine hardware, transmission equipment, and related software, including for cybersecurity.

## Help on the Horizon

In March, the Biden Administration announced a National Cybersecurity Strategy that seeks to "build and enhance collaboration around five pillars:"

1. **Defend critical infrastructure, which includes hospitals**
2. **Disrupt and dismantle threat actors, develop a federal approach to ransomware, and engage the private sector in disruption activities**
3. **Shape market forces to drive security and resilience, which includes federal grant programs to promote secure and resilient investments in new infrastructure**
4. **Invest in a resilient future through strategic investments and coordinated, collaborative action**
5. **Forge international partnerships to pursue shared goals**

Significant strides have already been made in the form of legislation or pending legislation aimed at bolstering our national cybersecurity workforce, including initiatives that incentivize students to pursue careers in healthcare. And it appears that more help is on the way.

The pressing cybersecurity challenges facing hospitals and health systems have garnered recognition at the highest echelons of government, resulting in additional federal support. However, it's crucial to acknowledge that solutions to these issues cannot solely rely on government intervention. Leveraging the available resources, including those mentioned above, is an important step toward strengthening your organization's cybersecurity defenses and protecting healthcare in our communities.

Kate has had over 21 years of experience in healthcare with specific experience in small, rural, and not-for-profit healthcare organizations. She is very familiar with the continuous struggles within these facilities to do more with less. Kate was the CIO and CISO for a Critical Access Hospital & Health Center, and developed the security program from scratch, including governance model, strategic planning, security control selection, and implementation. Kate has been working with HSCC and 405(d) to further the cause of cybersecurity in healthcare. She is a champion for federal and state funding for cybersecurity in small, rural, and not-for-profit organizations.

# HICP in the Spotlight

The HPH sector is increasingly targeted by ransomware attacks due to its valuable PHI. To safeguard this critical infrastructure, a security posture focused on identity management, access control, and data security should become part of daily operations. One proposed solution is the zero trust security strategy.

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. The strategy provides guidance for organizations to protect their resources by creating processes and workflows focused on protecting assets and securing sensitive data. Building a zero trust architecture that encompasses multi-layer protections strengthens your security posture. This means all device and user identities, both internal and external, are validated prior to being granted access to network resources.

This approach can be used to mitigate vulnerabilities created by network trends, including bring your own device (BYOD), cloud-based services and users working remotely. Your organization can enable the zero trust strategy at all network levels to ensure a strong security posture and this includes firewalls, physical security, and all IT systems and their users. Employees should also be trained on email security and how to recognize phishing attempts.

One way to begin implementing zero trust into your healthcare organization includes applying an access and identity management solution. (This practice can be found in Cybersecurity Practice #3: Access Management located in Technical Volumes 1 and 2.) Applying a least privilege access process creates additional security controls by only allowing users access to applications they need to do their work. For example, a front desk receptionist should not be able to view/edit the same level of PHI a physician can. This process can be automated to grant file and data access applicable to each job function. It also ensures that when an employee changes jobs or leaves the organization, their access is revoked. This prevents any additional vulnerabilities that might arise when access control is not continuously monitored. This is just one way of implementing zero trust in your organization; one that the practices covered in HICP can help your organization achieve.

*Your organization can enable the zero trust strategy at all network levels to ensure a strong security posture. The Health Industry Cybersecurity Practices 2023 Edition can help you implement this strategy in your organization. For more information, checkout our website at 405d.hhs.gov.*

# Unprepared for Long-Term Outages? Your Organization Could Face More Than You Realize!

**By: Donna Grindle and Gerry Blass, 405(d) Task Group Members**

*The 405(d) Chronicles is a platform for sharing firsthand insight, lessons learned, and perspectives from cybersecurity professionals in the field today.*

Investing in disaster recovery, incident response and business continuity plans is a wise investment for organizations that will ensure great returns through resiliency and risk mitigation. These three plans working side-by-side provide the optimal conditions to foster organizational resilience. Ensuring uninterrupted operations in healthcare organizations is crucial, particularly as they can significantly impact patient care and safety. Additionally, such events can result in severe economic losses, such as revenue reduction, data corruption, and reputational harm. As the duration of the disruption increases, it becomes increasingly vital to have a comprehensive plan that covers various outage scenarios. By investing in incident response and business continuity planning that considers long-term effects, organizations can mitigate the impact of disruptions and demonstrate their capability to provide consistent services regardless of circumstances.

## Incident response and business continuity plans matter as much as disaster recovery plans

Disaster recovery (DR) is often the primary concern when an organization's planning is brought up. "Do we have a backup?" This question comes to mind for many of us when anyone mentions planning for things to go wrong. However, incident response (IR) and business continuity (BC) plans are as crucial as disaster recovery when preparing for the inevitable need for recovery.

IR plans help organizations identify, contain, and resolve any incident or breach promptly and efficiently. These plans include detailed procedures outlining the steps to be taken during an incident, including communication protocols, roles and responsibilities of personnel involved, identification of critical assets or systems to protect, etc.

BC plans ensure that essential functions of the organization continue to operate during an unexpected disruption. Business continuity planning involves identifying critical processes within the organization and developing strategies for temporary operations during a disruption until complete disaster recovery can be accomplished.

Together, these plans provide a comprehensive approach to organizational resilience, ensuring that organizations can face unexpected disruptions head-on and continue to provide services to their patients, clients, and customers during disruptions.

## The threat of long-term outages

These outages can be caused by various factors, including natural disasters, cyber-attacks, equipment failure, power failures, or even global events like pandemics. These disruptions can last for several days, weeks, or even months.

Long-term outages can be a significant threat to organizations, especially those that rely heavily on technology as we do in healthcare today. In today's digital age, most businesses depend on technology to operate efficiently and effectively. However, when an outage occurs and lasts for an extended period, it can cause severe disruption in the workflow.

## Potential impact on an organization

The potential impact on an organization from long-term outages can be catastrophic.

The inability to access critical systems or data for all businesses can lead to revenue losses, missed deadlines, data loss or corruption, reduced customer satisfaction, long-term reputation damage, and loss of trust.

The risks and consequences of being unprepared for long-term outages in healthcare organizations are more significant than many other risks. Yes, they experience all the issues as others. Most importantly, though, the possible impacts on patient care and safety are severe, potentially leading to long-term health issues and even loss of life.

## Importance of a comprehensive plan

The longer an outage lasts, the more it can cost to bring systems back online. This is especially true if data is lost during the outage and must be recovered or recreated. A comprehensive plan is crucial for organizations to mitigate risks associated with long-term outages. It helps ensure business continuity by guiding how to respond effectively in different scenarios while

minimizing the impact on patients, clients, revenue streams, and reputation.

## Key components to address long-term outages

Comprehensive plans should include contingencies for various scenarios leading to an outage. This ensures you have backup systems that will help minimize downtime while ensuring critical business functions continue during any potential disruptions.

The plan should outline the roles and responsibilities of key personnel during such events and provide clear guidelines for communication with stakeholders, including employees and customers. This will help minimize confusion and prevent panic among employees while ensuring that customers/patients/clients are kept informed about any potential disruptions to services they rely on.

Organizations should consider partnering with experts who can provide specialized expertise during a long-term outage. This could include disaster recovery specialists or energy consultants who can offer guidance on maintaining operations during an extended outage and developing strategies for future resilience. By addressing these key components, organizations can help mitigate the risk of long-term outages and ensure they are prepared to weather any storm, including digital ones.

A recent study found that impacts on one healthcare organization in an area will also affect others. Your plan should include contingency plans for overflow being sent to your organization due to problems in any others nearby. See: Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US

## Training, testing, and updating the plan regularly

This plan must be periodically updated and communicated to all relevant stakeholders. One of the most critical aspects of any IR/BC/DR plan is testing and updating it regularly. Testing your plan allows you to identify weaknesses and gaps in your preparedness strategy, which can be addressed before an emergency occurs. It also ensures all employees know their roles and responsibilities during a crisis.

Regular updates to the plan are equally important as they account for changes in technology, personnel, or business operations. Since the last update, outdated plans may not reflect current circumstances or address new threats. The best approach is to review and update the plan at least annually or after any significant organizational change. Include these plans in your Security Risk Assessment (SRA) process that generally follows the same cadence.

Refraining from regularly testing and updating your plans increases your organization's risk of being ill-prepared for long-term outages. Inadequate preparation may result in extended downtime, lost revenue, patient/client/customer dissatisfaction, damage to reputation, or even legal liabilities. Therefore, organizations must prioritize these practices as part of their business risk management strategy.

## Conclusion: Preparing for the worst-case scenario must include the potential for disruptions lasting more than hours or days but also weeks and months.

Robust plans include steps on communicating with stakeholders during an emergency, restoring critical systems and services quickly after a disruption, and how employees should respond in an emergency. Organizations that invest time in designing adequate incident response and business continuity plans can minimize the impact of unplanned outages on their operations.

Incident response and business continuity planning must be encouraged by organizations that want to remain operational even during times of crisis. The benefits of having these plans outweigh the costs involved in creating them. A well-executed plan saves time, money, and resources while keeping customers happy by reducing downtime, thereby improving their confidence in the organization's ability to provide consistent service delivery.

You may never know whether or not your plans directly impacted patient care and patient safety, but we all must assume it will. Our healthcare sector has so many moving parts. Your organization's ability to protect patients from severe impacts is almost certain to matter somewhere down the line.

## Resources to help in your planning process

**HICP** - 405(d) - sign up for emails letting you know when additional assistance is released.

**HC3** - Health Sector Cybersecurity Coordination Center (HC3) | HHS.gov

**HSCC** - Operational Continuity - Cyber Incident (OCCI) | Health Sector Coordinating Council

**NIST** - NIST Recovery Webinar Slide Deck and Computer Security Incident Handling Guide

**Ready.gov Business** - Business | Ready.gov

**CISA** - CISA Tabletop Exercise Packages

# In Case You Missed It

The HHS 405(d) Program released a new poster helping everyone learn "How to Stay in the Cyber Safety Zone". This poster goes through each of the top 5 cyber threats as outlined in the *Health Industry Cybersecurity Practices (HICP) 2023 Edition* and provides everyone in a healthcare organization tips on how to mitigate them.

We encourage everyone to download the Poster HERE and place it in your workspaces.


# Other HHS Resources

## OCR

HHS Office for Civil Rights Settles HIPAA Investigation with Arkansas Business Associate MedEvolve Following Unlawful Disclosure of Protected Health Information on an Unsecured Server for $350,000

HHS Office for Civil Rights Reaches Agreement with Health Care Provider in New Jersey That Disclosed Patient Information in Response to Negative

## HC3

Healthcare Sector Potentially at Risk from Critical Vulnerability in MOVEit Transfer Software

## FDA

Illumina Cybersecurity Vulnerability Affecting the Universal Copy Service Software May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers

## HHS Cybersecurity Program

offers resources, including video training modules, designed to foster an enterprisewide secure and trusted environment.

### About The 405(d) Post

*This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The "A Word from the Task Group" and the "405(d) Chronicles" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter. The news articles are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.*

**Need To Contact Us?** Email us at cisa405d@hhs.gov

## Follow us!

Facebook Twitter

Instagram LinkedIn

**Visit our website at 405d.hhs.gov!**