Testimony of

Katherine (Kate) Pierce

Former Chief Information Officer & Chief Information Security Officer,

North Country Hospital

and

Current Senior Virtual Information Security Officer & Executive Director of Subsidy,

Fortified Health Security

Before the

United States Senate

Homeland Security & Government Affairs Committee

March 16, 2023

Introduction

Chairman Peters, Ranking Member Paul, and members of the Committee, my name is Katherine (Kate) Pierce. I served as the CIO and CISO for a Critical Access Hospital for over 21 years and I currently serve as a Senior Virtual Information Security Officer and Executive Director of Subsidy for Fortified Health Security. I want to thank you for this opportunity to address the Committee on Homeland Security and Government Affairs and provide an industry perspective on cybersecurity threats in the health sector, the current challenges small and rural healthcare organizations face, the dangers of exposing healthcare sensitive data to adversaries, and the impact to communities when healthcare organizations experience cyberattacks. I also herein respectfully submit recommendations on how this committee can assist healthcare organizations in improving their overall cybersecurity posture.

Background

North Country Hospital and Health Center, Inc.
North Country Hospital is a Critical Access Hospital (CAH) located five miles from the Canadian border in the Northeast Kingdom of Vermont. It offers healthcare services to the 27,000 residents in Orleans and North Essex County, as well as visitors who travel to enjoy the area's recreational resources. In its 100 years, the medical campus has grown to include fourteen clinics, including primary care, a surgical suite, obstetrics & gynecology, 24-hour emergency department, pediatrics, an intensive care unit, medical/surgical floor and branches for dialysis, orthopedics and sleep

disorders, as well as areas for radiology, laboratory and physical therapy. In addition, services are provided at four rural health clinics in Orleans County.

Fortified Health Security

Fortified is a leading national cybersecurity partner to thousands of healthcare facilities across the U.S., providing managed advisory and security services that help clients protect patient data and reduce risk. A recipient of multiple industry accolades, Fortified was recently awarded a second Best in KLAS award for Security and Privacy Managed Services. Since its inception, Fortified has works alongside healthcare organizations to build customized programs and processes that reduce risk and increase their security posture over time by helping them address challenges with human capital, technology and security best practices. Led by a team of industry-recognized cyber experts, Fortified publishes the nationally recognized "Horizon Report."

Fortified is actively driving the national conversation around healthcare cybersecurity. Its monthly Roundtables address current threats, new technology, and strategies to harden cybersecurity postures and address incidents. Fortified's experienced cybersecurity leaders are frequently interviewed and featured in national trade publications. And Fortified is also a member of the Cybersecurity Working Group of the Healthcare Sector Coordinating Council.

Current Cyber Threat Landscape in Healthcare

Recent Healthcare Cybersecurity Updates

The top cyber threats for healthcare in 2022 were phishing, ransomware, data breaches, and DDoS Attacks. While these threats were prevalent across the breadth of critical infrastructure, in 2022 healthcare continued to be the top focus, with 148 of the 649 cyberattacks on critical infrastructure targeted at healthcare organizations. There are multiple reasons for this, but two primary lines of thought are that healthcare data records are worth in excess of fifty times more than other records on the dark web (Industry Voices-Forget Credit Card Numbers. Medical Records are the Hottest Items on the Dark Web), and that, due to the time-sensitive nature of healthcare services, hospitals are more likely to pay the ransom (61% paid ransom in 2022) (The State of Ransomware in Healthcare 2022 – Sophos News).

Shift in Focus of Cyber Attackers

Another alarming trend that escalated in 2022 was cyber attackers shifting focus to small and rural hospitals. While most larger health systems have implemented advanced cybersecurity hygiene to thwart attacks and are employing large cybersecurity teams with sophisticated defenses, small facilities continue to struggle. In fact, there is a large disparity in cybersecurity spending when it comes to small- to medium-sized rural facilities. Sadly, this is not only well-known to hospital systems, but to cyber criminals as well. Fierce Healthcare reported in August of 2022 that "Smaller hospital systems and specialty clinics often lack the same level of security preparedness, staff size or budget and have weaker cyber defenses. Attackers are

continuing to push the envelope and change the playing field when it comes to healthcare data breaches and attacks. The move from large hospital systems and payers to smaller entities that have a deficit in their Cyber defenses shows a massive change in victims and approach. As we continue into 2022, we anticipate attackers to continue to focus on smaller entities for ease of attack, but also for evasion of media attention and escalation with law enforcement." This concept was reinforced by Healthcare Dive, stating, "Cyberattacks are pivoting to target smaller healthcare companies and specialty clinics without the resources to protect themselves, instead of larger health systems that – despite being treasure troves of personal and medical data – generally have more sophisticated security." The overall national risk for healthcare is compounded when we consider that the majority of smaller hospitals are connected to larger systems, so when cybercriminals attack the small facility, it is often the "path of least resistance" into much larger healthcare networks.

Increased Time to Recovery and Escalating Average Cost of Breach

The length of time required to recover from a breach increased, and the cost for recovery climbed to $10.10 million in 2022, with CommonSpirit reporting more than $150 million in recovery costs Healthcare and cybersecurity in the U.S. - Statistics & Facts | Statista. Both of these statistics are especially significant to smaller organizations, when considering an Expert Insight survey that showed the average recovery time is 33% longer for small organizations, and the cost per hour of system outage is 55% higher for this group than for hospitals over 1000 beds. Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know | Expert Insights

Current Challenges Faced by Small and Rural Organizations

Budget Constraints

Rural healthcare facilities are facing unprecedented economic challenges, which could quickly lead to a sharp decline in the number of hospitals available to our rural communities. When we consider the barriers to strong cyber programs, a Becker's Health IT article from December 2022 indicated that inadequate budgets are the number one issue keeping healthcare organizations from achieving more effective cybersecurity protections. This is especially true for small and rural facilities, with many facing severely strained budgets and danger of closure. Michael Topchik, national leader for Chartis, indicated this month that 43% of rural hospitals are operating in the red (Nearly Half of Rural Hospitals Are Operating in the Red, Study Says (dailyyonder.com), and a recent AHA Report outlines the closer of 136 rural hospitals between 2010 and 2021, with 19 in 2020 alone. The report indicated that in addition to lower patient volumes, rural hospitals often treat patient populations that are older, sicker and poorer compared to the national average. For example, a higher percentage of patients in rural areas are uninsured and 26% of uninsured, rural patients delayed seeking care due to cost. The Crisis in Rural Healthcare report indicates that, "More than 600 additional rural hospitals – nearly 30% of all rural hospitals in the country – are at risk of closing in the near future."

A few of the prevalent contributing factors to the economic distress of these rural healthcare providers include the severe shortage of clinical staff leading to significant

wage hikes, the increased need for scarce behavioral health services, a shortage of long-term care beds creating extended stays which are reimbursed at lower levels, and a sharp increase in supply chain and technology costs. Rural hospitals also tend to have lower overall reimbursement rates, which is projected to worsen as the end to the PHE takes effect, with as many as 15 million Medicaid patients anticipated to lose coverage (The End of the PHE: How Providers Can Cope With the Impact of up to 15 Million Medicaid Enrollees Losing Coverage (beckershospitalreview.com)). With the large number of competing priorities within these small health systems, it is difficult, if not impossible, to focus on cyber defenses. Budgets are strained, and with cybersecurity not seen as a priority for small and rural hospitals, cyber initiatives are often some of the first items cut from operational and capital budgets.

Security Staffing

Cybersecurity staff resources nationally are in high demand, and this shortage of cybersecurity skilled professionals is not ending anytime soon. According to the 2022 ISC2 report, "Despite adding more than 464,000 workers in the past year, the cybersecurity workforce gap has grown more than twice as much as the workforce."ISC2-Cybersecurity-Workforce-Study.ashx. I have had the opportunity to interact with small and rural hospitals across the counter, and most facilities have little to no trained security personnel on staff. Every member of the organization wears multiple hats and is spread extremely thin. The IT teams are generally very small (2-8 FTEs) and they can barely keep up with day-to-day help desk tickets. This small group of staff often needs to support more than 200 different information systems,

hundreds of interfaces, servers, laptops, desktops, printers, mobile devices, phone systems, internet connections, access control, biomedical devices, imaging devices, and all the other technical components that keep hospitals running. It becomes quickly apparent why cybersecurity initiatives take a back seat to the day-to-day business of keeping the facilities running. A basic security measure like 24/7 monitoring of systems is "pie-in-the-sky" for these organizations. Despite all the guidance, recommendations and services provided over the past few years by HSCC, 405(d), H-ISAC, CISA and other organizations, I have found that the vast majority of small and rural hospitals are unaware of these resources, and too overwhelmed to take advantage of these valuable tools. They are treading water, only addressing issues that are necessary to keep the clinical operations functioning or are mandatory.

Small hospitals especially struggle to recruit and retain security staff, with current salaries for these high-demand professionals beyond the already strained budgets. Many facilities attempt to train staff from within, but often these staff members quickly leave for other higher-paying jobs outside the organizations.

Technical Debt

Small and rural hospitals also typically have an abundance of technical debt, with many outdated systems that they cannot afford to keep updated, including hardware and software that is beyond end-of-life. While COVID greatly expanded the digital footprint of most hospitals, with new systems to meet the needs for telehealth and remote workforce implemented at warp speed, often very little consideration was

given to security. These factors contribute to the increased attack surface for small hospitals when compared with larger facilities.

Cyber Insurance Coverage

In recent years, it has become increasingly difficult for small rural hospitals to rely on cyber insurance coverage to assist them in recovering financially from an attack. Insurance companies have become much more selective in extending coverage, making it difficult for smaller organizations to meet their stringent requirements. If hospitals do qualify for coverage, often rates are 35-75% higher than larger entities, with lower limits, and more exclusions. Relying on cyber insurance to offset these risks is quickly evaporating as an option.

Summary

The topics listed above are not anywhere near exhaustive, but these items, in my opinion, combine to create a significant increased risk for cyberattacks for this segment of the healthcare sector, with the risk anticipated to continue to grow as the threats increase.

Dangers of Exposing Healthcare Sensitive Data to Adversaries

Protected Healthcare Information (PHI) is a concern well beyond HIPAA mandates. For a patient, their data is highly sensitive, and a leak can be extremely damaging. Healthcare data is extremely rich including Protected Health Information (PHI), Personally Identifiable Information (PII) and Payment Card Industry (PCI) data. When attackers can extort all three of these types of information, it is evident why healthcare data remains the information most targeted by cybercriminals across all critical infrastructure sectors. Healthcare records remain the most valuable information on the dark web (https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web). But beyond the impact to healthcare organizations of reputational harm, loss of staff, difficulty in recruiting future staff, insurmountable recovery costs, legal penalties, and both civil and criminal lawsuits, the far-reaching ramification to patients of a security breach can be devastating. Exposure of health information can lead to individual reputational harm, identity theft, extortion, monetary loss, and patient safety risks.

Impact to Communities When Healthcare Organizations Experience Cyberattacks

Diversion of Patients

The impact on rural communities during a cyberattack is hard to overstate. While attacks in urban areas are also impactful, populated areas provide other healthcare options for patients close by, lessening the potential for patient safety issues. In most rural areas, the next closest healthcare facility may be 45 miles away or more. This can make the diversion of patients infeasible. With recent attacks causing outages measured in weeks, and sometimes months, the impact on patient safety is easy to comprehend when travel times can take up to an hour or more. This delay can directly influence negative outcomes for many healthcare issues such as stroke, heart attack, sepsis, or even the delivery of a child. When patients are diverted, nearby facilities can become overwhelmed beyond capacity, creating a cascading crisis throughout the community. This is supported by a University of Washington study showing the closure of urban hospitals had no impact on their surrounding communities, but the closure of rural hospitals had a mortality rate increase of 5.9%, primarily due to increased travel times for patients (Rural hospital closings cause mortality rates to rise, study finds (nbcnews.com).

Hospital's Reliance on Electronic Health Records

Since the HITECH Act of 2009, more than 97% of hospitals in the US have adopted Electronic Health Records. They have integrated these systems and workflows into every aspect of safe, efficient, effective patient care and are highly dependent on

these systems to maintain the high-quality standards of care that patients deserve. When these systems are not available, hospitals are significantly hindered, which can lead to a sharp increase in the likelihood of patient harm.

The effect on patient safety when systems are offline is very evident. A report from a recent cyber incident detailed a litany of issues that prevented staff from caring for patients. Some of the most sobering effects were that patient safety checks within the EHR (Electronic Health Record) were not available, paper documentation significantly slowed processes for workers, with no registration system, patients "slipped through the cracks," ambulances quickly became backed up as crews waited to hand off patients, lab results were delayed for hours (routine lab tests taking up to 13 hours and STAT tests up to 5 hours), and medication delivery safeguards were not available. Additionally, communication between departments was slow and manual, clinical staff had no access to patient history (many patients do not know their medications or allergies), personnel could not access contact information for family members or advanced directives, leading to staff not knowing whether to resuscitate a patient. The manual paper charting workarounds were woefully insufficient, with illegible handwriting in paper charts and many staff that had never been trained in how to document care on paper. Ultimately, an ED nurse at this facility called 911 to ask if fire department support could be dispatched to support the Emergency Department because they were so overwhelmed.

All of these items contributed to the decreased level of patient care at this facility, and any one of them could lead to significant patient safety issues.

Community Health and Financial Impacts

While the patient safety concerns may be more easily understood, the closure of a hospital can place additional strain on other healthcare services within the community or in surrounding communities. Neighboring hospitals can be overwhelmed if diversion occurs, facilities that are connected via virtual private networks will need to be vigilant to avoid becoming a subsidiary victim, clinics or other health systems that typically receive results could see significant delays, and communication can become challenging, both between the hospital and their patients and between other healthcare providers.

In addition to the recovery costs for these organizations, it is common for hospitals to see lower reimbursement due to decreased volume and inability to capture costs. Reputational harm can also have significant impact on finances, with legal penalties, civil lawsuits, and other recovery costs potentially all contributing to a hospital's inability to recover from a cyber event given their already strained budgets.

Summary

Diversion of patients causing excessive delays in care, our national overall reliance on electronic health records to safely care for patients, and the overall community and financial impact are all very real, well-documented results of the growing cyberattacks on our nation's health sector. While the example above used may appear extreme, it can very easily be replicated in any of the 1796 rural hospitals across the country that are not prepared for these events.

Recommendations For Assistance to Improve Cybersecurity Postures for Small and Rural Hospitals

Recommendation 1: Minimum Security Standards

In small and rural hospitals, there are always many competing priorities for time and money. Without minimum standards, these facilities will not prioritize cybersecurity over the seemingly more pressing needs in currently strained budgets. However, whichever cybersecurity minimum standards are imposed, they must be reasonable, achievable, and continually evolving as security needs develop. Consideration must be given to the limitations of small and rural hospitals, and the potential negative impact new requirements could have on these organizations.

My recommendation would be to start with the following requirements, based on the items outlined in the Health Industry Cybersecurity Practices (HICP) document. These could be grouped into five basic categories, as outlined below.

1. Email Security & Protection (This is the biggest risk)
    a. Strong filtering / blocking systems with best practice controls implemented (like blocking macros, not allowing .exe files, geo-blocking, etc.)
    b. Security awareness training (including phishing simulation, regular training, etc.)
2. Access Management (Sites must know & manage who is on the network!)
    a. Role-based security
    b. Strong Password Management
    c. Multifactor Authentication

   d. Provisioning/Deprovisioning best practices

3. Asset Management – (Sites must know & manage what is on the network!)
   a. Inventory management
   b. Asset tracking
   c. End Point Protection
4. Network Management – (Sites must manage the gateway and keep things patched to prevent holes)
   a. Firewall configuration best practices
   b. Regular patch management
   c. Change/Configuration Management best practices
   d. Data protection and loss prevention
5. Incident Response – (Must have a plan for when they get hit)
   a. Documented IRP plan
   b. Regular exercises
   c. Disaster recovery plan

<u>Recommendation 2: Funding/Incentives</u>

The minimum standards outlined above can be reasonably expected of all facilities, but not without assistance from the federal government for small and rural facilities. Assistance should be made available in a variety of ways. The pros and cons of each option are outlined below:

Subsidies:

Subsidies are very effective for smaller hospitals. We have seen the positive effect of the USAC Health Connect Fund which allowed for small and rural healthcare organizations to reduce the costs of internet and telephony services by 65% since 2012. This is a very active fund, and most rural facilities (and clinics) are taking advantage of the cost reduction available for these services. Currently, this fund is restricted to items that affect the core and wide area network (WAN) only, but it does include some limited equipment and network management items. An effective way to quickly implement subsidies would be to increase the scope of the existing Health Connect Fund to include cybersecurity initiatives that are aligned with any minimum standards imposed. This could greatly reduce the cost of services of implementing cyber standards, and the funding would be repeatable year over year to continue to grow cyber programs as the needs change. Alternatively, if USAC cannot support this fund's expansion, implementing a similar subsidy fund through HHS or FEMA to address cybersecurity needs would have a positive impact, too.

Grants:

While grants can be very effective, it should be noted that most small organizations do not have grant writers on staff, and do not have the capacity to respond to complex grant applications or maintain the detailed tracking of information that many grants require. Existing grants under Homeland Security for cybersecurity are targeted at specific groups, such as state and local, tribal, law enforcement, or houses of worship. This makes it difficult for small and rural facilities to be competitive for these funds. If grants are an option under consideration, they need to be specific to

small and rural healthcare organizations (which is the biggest risk sector), be allowed over a period of three to five years to ensure adequate time for implementation of security given resource constraints, have a low application burden (similar to COVID funding where the funds were dispersed with proof of utilization coming later or the return of the funds), and have a reasonable threshold of ongoing administrative requirements.

Meaningful Security (Similar to Meaningful Use)

The Meaningful Use program was proven to be very effective in moving hospitals to electronic health records. However, the program was administratively burdensome for many small organizations. If a "Meaningful Security" program were used to incentivize hospitals to build their security programs, it would need to be specifically targeted to small and rural facilities, since this is the group that is most in need of assistance. Also, consideration would need to be given to how cybersecurity partners would become eligible under the program (similar to the CEHRT program for MU). One drawback to this type of incentive is the delay in getting this funding to facilities due to the administrative work it required to develop and implement the program. Many facilities could close before this becomes available.

Enhanced CMS Payments:

Another option to assist small and rural hospitals would be to enhance CMS payments to offset the costs of cyber programs, with a requirement for the submission of evidence to indicate that the excess funds were spent appropriately.

This may take additional time to design and implement, as there would need to be a clear definition eligible items, vetting (or certification) of software and services that qualify, a determination of how to qualify (ensuring that the neediest of our hospitals are able to take advantage of the funding), and other administrative decision points.

Recommendation 3: Coordination of Government Efforts

There are several agencies within the government trying to solve the cybersecurity challenges our nation is facing. While these efforts are greatly appreciated, the lack of clarity on who is ultimately leading healthcare cybersecurity can be unnecessarily confusing for small organizations. While the guidance and services available to date from a variety of organizations, such as HSCC, 405(d), ASPR, H-ISAC, CISA, and other organizations are a positive step, my interactions with smaller organizations have shown that the majority of small and rural hospitals are not aware of the recommendations, guidance, or service offerings. Additionally, even when these options are presented, small hospitals do not have time to consider engaging or implementing the resources as they do not have the staff or the knowledge to move forward. Without minimum requirements and incentives, these great tools could be overlooked by the organizations that need them most.

It should also be noted that many of the services currently available do not take into consideration the "healthcare-specific" nuances of cybersecurity. While CISA has many great services available, when engaged, it quickly becomes apparent that resources at CISA may not understand how healthcare systems operate, and how this

affects their ability to quickly implement security controls. For example, in many industries it is standard to apply system patches as soon as they become available. But in healthcare, due to the potential negative impact to patient care, patches are slow to become available and must be thoroughly tested prior to application, with a detailed change management plan. Many times, patching involves vendor associated costs that must be budgeted due to ensure the correct level of expertise required for the complex interfaces and equipment involved.

The recommendation here is to have one agency (preferably HHS) take the clear lead on all healthcare-specific cybersecurity needs and engage other agencies to ensure they are well versed on healthcare cybersecurity nuances. Alternatively, if CISA, Homeland Security, USAC, FCC and other areas are engaged in healthcare cybersecurity, they need to collaborate with HHS to ensure there is a comprehensive understanding of healthcare-specific cybersecurity management.

Recommendation 4: Allow Declaration of Emergency for Cyber Attacks on Healthcare

Cyber-attacks are a leading cause of hospitals not being able to effectively provide care to patients. The challenges that current exist with cyber insurance leave many organizations at risk of not being able to recover from a cyber event. Cyber-attacks should be handled like other hazards, allowing facilities to take advantage of resources available under a declaration of emergency. Establishing a FEMA cyber disaster relief program would provide victims of these attacks access to emergency-related assistance. This would not conflict with current cyber insurance coverage,

rather enhance the coverage and would allow for faster recovery and increased financial stability for health systems.

Conclusion

Currently, the cyber attackers are winning the battle. The Cybersecurity Act of 2015 is now approaching eight years old. While there have been many advancements made with respect to published documents, services, and guidance, we have continued to lose ground to these cyber criminals. There must be a bipartisan plan to address this cybersecurity crisis immediately. We can no longer delay without further jeopardizing our healthcare system, especially the small and rural hospitals that are already in crisis.