MEDICUS IT

How Smart Community Health Centers Protect Themselves... Online, That is

A CHC cybersecurity guide from Medicus IT

Cybersecurity. Everyone knows it's essential. No one likes having to implement or manage it. And yet, community health centers (CHCs) need to look at cybersecurity as an opportunity – both for winning federal grants and as the foundation for IT that streamlines operations and prepares the organization for future growth.

Here's a quick guide for how your organization can look at cybersecurity from a fresh perspective that improves protection, stability, and continuity while simultaneously minimizing expense and intrusion into daily operations.

Adjust Your Mindset

Many CHCs look at cybersecurity from a cost perspective. In truth, cybersecurity should be evaluated in terms of its value:

How much will it cost your CHC if a ransomware prevents operations for a day? A week? A month?

What happens if a security breach impacts your ability to secure or retain governmental block grants?

What are the legal liabilities if patient information leaks outside the organization?

Increasingly, CHCs that invest in security gain advantage over other organizations that don't. It doesn't need to be overly complicated, but it must be taken seriously and addressed strategically to be efficient and effective.

Understand What You're Protecting

Cybersecurity means different things to different people. For CHCs, cybersecurity begins by directly addressing these elements, all of which are fundamental for grant applications:

Devices and Networks – Every device and internal network must be hardened against attack and secured from unauthorized access.

Privacy – Patient, payer, provider, and financial information must carry appropriate access and distribution controls so that only authorized individuals may reach, use, print, or transfer sensitive information.

Digital Identity – Every individual or organization with access to sensitive data must be vetted to ensure proper levels of privilege, especially when new employees or partners onboard or lose their connection to the CHC.

Third-Party Connections – Your CHC only can protect itself – you cannot be responsible for security practices at other organizations. You can, however, insist on certifications and audits proving that every third-party connection mitigates your trusted relationship with proper risk management practices.

Reputation and Viability – Any digital breach of trust leads to negative publicity. What healthcare organizations often fail to understand is the wider range of damage. Years of care, business, and personal relationships immediately come into question. Every instance of leaked or lost information becomes the grounds for potential legal or regulatory financial penalty. Senior management may carry personal risk of fines, loss of job, or prosecution. This damage may take years to mend or may never be fully repaired.

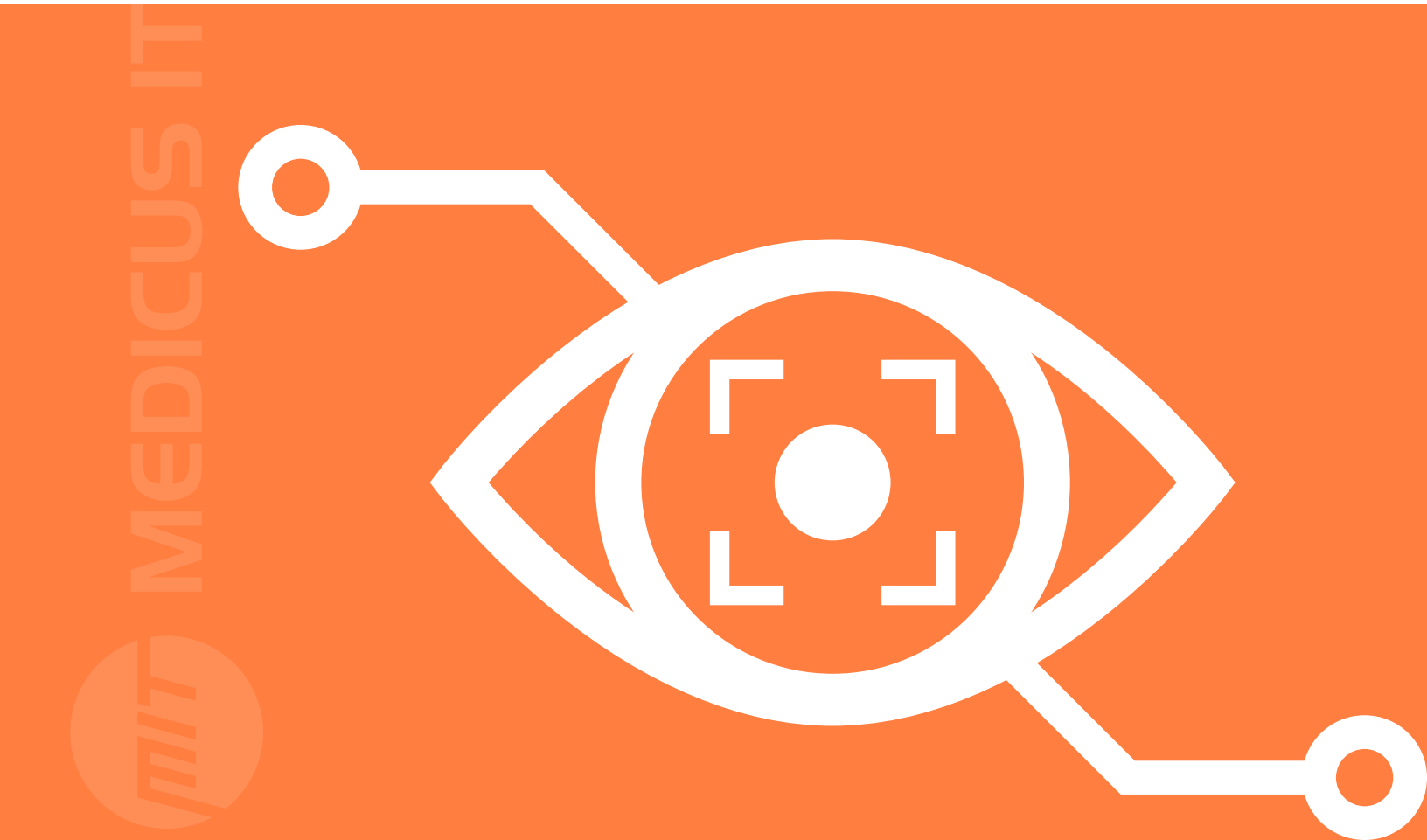
Outsource Your Infrastructure to A Trusted Healthcare IT Partner

As the previous section illustrates, CHC cybersecurity quickly gets complicated. Given the range of practice types and the scope and scale of operations at a typical CHC, protection all these elements require considerable expertise. Every dollar spent building this infrastructure represents money and man-hours not focused on patient care.

That's why many CHCs rely on third-party IT vendors, trusting that these outside entities understand the healthcare cybersecurity complexities inherent in organizations that deliver services ranging from basic care to population health, from dental to PT and rehab. Basic questions every CHC needs to ask these organizations must include::

How do you make multifactor authentication (MFA) easy for every one of our employees to unsderstand and use? – MFA means using a code or a token that plugs into devices to ensure someone is authorized to access that system, with only the privileges they need to see only the information they need to do their jobs.

Do you provide secure DNS? The Domain Name System is the "address book" that the internet uses to enable communications between devices, applications, and networks, so that every one of your systems and can connect to third-party organizations. You need to insist that all internet traffic at your CHCs route traffic securely and anonymously, without leaking data or enabling unauthorized personnel from stealing confidential data.



What are your proven, guaranteed provisions for data backup and emergency restoration? This last topic seems simple, but many CHCs fail at this most basic of functions. And yet, nothing cripples a CHC faster or with more devastating effect than when critical data disappears due to equipment failure, power outage, or successful ransomware or other cyberattack.

In short, these elements require not just superior IT, they demand healthcare IT – a partner who understands how to provide secure infrastructure for the unique demands of CHCs, with a proven record of success at organizations of all sizes, anywhere in the country.

Test, Test, Test, Test, Test

Prospective IT services vendors often offer security assessments and even training as part of their offerings. That's a bad idea. No vendor should have that conflict of interest, in which they install and maintain the same systems they assess for risk and performance.

Instead, split those functions across two separate partners – one who knows how to build secure healthcare IT, and one who knows how to provide regular, comprehensive security and risk management assessments. Better yet, make sure those two organizations are comfortable working with each other, so that your IT provider understands how to fix any vulnerabilities found via audit and assessment and provide appropriate training to your staff.

Key areas for regular and as-needed security audit include, but certainly aren't limited to:

- Administration rights and privileges
- Physical access controls
- Systems configurations and vulnerabilities
- Antivirus and intrusion prevention effectiveness
- Patching and update documentation
- Policies and procedures, including training achievement and retention
- Forensic analysis in case of a security threat or breach

Got Questions? Talk to Medicus IT

CHC-driven healthcare IT and security can easily become overwhelming. After all, your organization exists primarily to help people live healthier and more fully. IT and cybersecurity, however essential, shouldn't be your top-line, day-to-day concern.

That's where we can help. We're Medicus IT. We specialize in CHC-specific hybrid Cloud and on-premises solutions that install easily and rapidly establish secure operations for your team. Better yet, with more than 50 current CHC clients, we understand what it takes to transform and protect communities, one patient at a time. And, with more than 35 years specializing in healthcare technology, we have the breadth and depth to deliver.

Build the foundation for lasting change in your community and in your CHC, with no-worry, secure IT that delivers tight cost control, a superior patient experience, and demonstrable improvements in care. Contact Medicus IT today.

Together, we drive healthcare forward™

MEDICUS IT

For more information please visit us at MedicusIT.com

MEDICUS IT