THE TOP 4 SECURITY ISSUES FOR AMBULATORY PRACTICES IN 2024

As we head into 2024, ambulatory practices are hitting the ground running with everything from new patients and staff members to new technologies and requirements. However, four key security issues have already emerged, and practices that fail to pay attention run the risk of putting sensitive data at risk:

MEDICUS IT

1 SHADOW ELECTRONIC MEDICAL RECORDS

The massive migration of EMRs to the cloud offers significant benefits to practices. It also enhances opportunities to leverage third-party products and APIs to enhance the traditional EMR's capabilities. However, with this expanded capability, it is important to also account for the potential risks. As our employees interact with these new tools and the data they provide, we see personal health information (PHI) sprawling across the organization in places like file shares and emails, enhancing the ability to transmit or share protected health information to people within or even outside of the organization.

The motivation behind these "Shadow EMRs" is likely benign. But the best of intentions – for instance, to use data efficiently in a way that goes beyond what the EMR allows – poses a significant security risk. And it requires highly specialized healthcare security expertise to recognize these situations before sensitive or HIPAA information accidentally leaks.

2 THE NEED FOR A CULTURE OF SECURITY

Your staff members are busy. So busy that they may not see security and accountability as core to your operations. Indeed, they may imagine that security and accountability are technological concerns – handled by things like passwords and firewalls.

They don't realize that they pose the greatest risk to your systems security by through everything from phishing scams to leaving passwords visible on sticky notes. Building a culture of security that recognizes and overcomes these dangerous behaviors has never been more crucial.
And yet HOW to make that happen is challenging, even for the experts.

3 YOUR PARTNERS' SECURITY (OR LACK THERE OF)

Your partners may have systems that connect with yours for things like clinical interfaces, reporting, supplies, staffing, financial services, and more. And if their systems are compromised, your practice and its data can feel the impact in ways that extend all the way to a breach of Personally Identifiable Information, which can affect HIPAA compliance. When evaluating supply chain partners, it is critical to take a hard look at the measures they have in place to protect you. But who has the time to build those skills and take on that task?

4 THE ALLURE OF A.I.

Artificial Intelligence – in the form of Chat GPT, Bing, and a plethora of other emerging and evolving services – promises to speed analyses and reduce tedium (e.g., "Summarize all clinical summaries of physicians in our health system who prescribed Azythromycin this year.")

However, what most people don't understand is that data shared with the AI system might become part of its library – right down to the most sensitive patient information. And, since this technology is only going to grow and become more powerful, it is more essential than ever to train your people to safeguard your data. But how – especially given how rapidly A.I. and its applications are evolving?

These are complex topics – which no practice or practice group should tackle alone. You need a healthcare technology partner that understands how security impacts medical practices.

Only one organization has the healthcare and technology expertise to do it. Contact Medicus IT today for a Virtual Technology Executive consultation. We'll tell you how we can build the plan you need to improve your security quickly and affordably – so you can get back to what you do best – taking care of your patients.

For more information please visit us at MedicusIT.com

MEDICUS IT