HEALTHCARE DATA SECURITY CHECKLIST

SYSTEMS SOLUTIONS

The Risk:

Accuracy of medical records could mean life or death for a patient. But the transfer to digital platforms for private medical information is creating an international platter of possibility for hackers.

Patient portals are being added online for convenience to patients. New computer and tablet systems are added to nurse and doctor routines. Health Insurance is being bought and medical visits documented online. With these changes comes an added vulnerability.

These digital records are meant to help with accuracy and response time. They're meant to help patients live a healthier life and be more involved with their own health care.

But, as more information is stored online or in electronic form, the more we continue to hear about cyber attacks.

Within the last 5 years, criminal cyber attacks have increased by 125 percent inside the healthcare industry, according to a recent study from the security research firm Ponemon. According to respondents, on average they have dealt with almost 1 attack per month over the last year.

The scarier statistic is that ***26 percent of respondents were not sure*** if they had experienced an incident where patient information had been lost or exposed.

The Danger:

Understanding the risk and dangers an unsecure network poses is vital to taking the necessary steps to secure your network. Here are two dangers stolen medical data can pose, based on Ponemon research:

- It can put patients' lives at risk. If a hacker uses the stolen medical identity or deletes/changes any information there, it can have life threatening consequences. Inaccurate medical records can lead to a misdiagnosis or prescription errors.

- It can lead to a loss in trust of medical professionals. Healthcare professionals are there to help care for patients. But the level of help they are able to give, begins and ends with the trust built between patient and medical professional.

The Facts:

Cyber attacks are costly for both the healthcare system and the patients. And can be highly profitable for hackers. According to Dell SecureWorks, medical information is worth 20 times the price of a stolen credit card number.

In January and February of this year, more than 300,000 people's digital medical information has been exposed or stolen. Of those, over 50,000 were due to a hack or IT incident. It's important to note, these numbers only include breaches impacting more than 500 patients' information.

Once a breach is detected, it's a long and costly road ahead.

In early February, a L.A. hospital's entire computer system was locked down by hackers. To regain control of their system, they paid a bitcoin ransom equivalent to almost $17,000. So far, they do not believe any patient data was stolen. However, it was about 10 days before their system was fully restored.

How costly is it for the victimized patients? According to Ponemon's study on average, patients have had to spend $18,660 to restore their medical identity. This includes:

- paying for medical services performed on the thief
- legal counsel
- out of pocket costs due to lapse in insurance coverage after the theft

Your Security Checklist:

The threat is real. The consequences are high. But, there are ways to be prepared and keep a closer eye on your network. Here is a Security Checklist ***every*** healthcare organization should be examining multiple times a year:

1. **Perform a risk analysis for your organization and network.**
2. **Create a HIPAA client policy.**
3. **Create procedures based on the policy.**
4. **Create supporting documents for those procedures.**
5. **Have an outside IT source perform a perimeter security scan.**
6. **Have certified ethical hackers perform a network intrusion detection service.**
7. **Perform a website vulnerability scan; specifically targeting patient portals.**

Diligently completing this checklist is just the beginning of keeping your system secure. The policy, procedures and supporting documents must be used regularly. Creating a policy without follow up action will not keep anyone's information safe.

Systems Solutions can help you check off all of these items. Our procedures can keep your patients' data safe and help you stay HIPAA compliant so you can focus on your patients' health and not their data security. Our team will provide you with a risk analysis, a remediation plan and perform perimeter scans twice a year.

Call **270-444-9616** to learn more.