The importance of Cybersecurity in This Era of Radiology

Continued digitization has brought tremendous benefits to health care, making the industry more connected and efficient than ever. However, with an overwhelming number of data and patient records located on interconnected networks, the importance of actively protecting it all cannot be overstated. Hackers have continually evolved and adapted with technology. They are always seeking new sectors to attack, including in the health care space.

For radiology departments, the risks of experiencing cyber attacks has increased over the past several years with the profession becoming a mainly digital practice and widespread industry consolidation. With many radiologists now working remotely due to COVID-19, hackers are more likely than ever to jump at the opportunity to breach private data with employees working on mobile devices on less secure wireless networks.

Practices must begin to invest in and strengthen their cybersecurity immediately to prevent the possibility of an attack. As our industry transitions to a more virtual environment, taking immediate action may save the future of your practice and, more importantly, the future of your patients.

Understanding cyber attacks on health care practices

The incredible growth of industry technology has enhanced the medical profession, making data and information instantaneously accessible. However, this immediate access to

private data also creates opportunities for hackers to invade organizations' systems, majorly affecting the entire industry.

Cybercrimes cost the health care industry around $6.2 billion annually, with organizations individually losing an average of $3.7 million. There are also many other costs organizations could face with cybercrimes, including post-breach costs, potential fines from HIPAA and even lawsuits. What's more, employees can be major contributors to potential network breaches as well. According to a 2016 report from BakerHostetler, 24% of health care data breaches were the fault of employee errors.

Organizations are not the only ones affected by cyber attacks, however. Their patients suffer just as much, and in some cases, even more so. In 2019 alone, more than 40 million people were affected by health care data breaches, doubling the amount recorded in 2018. This trend is expected to increase as more data and protected health care information (PHI) becomes digitized on network servers across the industry.

Knowing where hackers will strike

It's hard to predict where hackers will attack next and how they will do so. Cybercrimes can stretch from breaching systems for patients' PHI, infecting networks in malware attacks or deliberately tampering with images and scans in ransomware attacks. This uncertainty can make securing data and preparing systems for attacks a challenging process.

While there is uncertainty in exactly how hackers will attack, they have been pretty consistent in targeting small and medium sized medical practices. This is because many of these specific practices don't have the manpower nor financial resources to field a full cybersecurity team, making their data less secure and easier to breach.

Hackers have also become interested in targeting health care networks consisting of consolidated practices. With scans, patient information and other data streamlined across multiple networks and facilities, there are more opportunities for hackers to breach, steal and manipulate private data.

Figuring out how practices can prevent cyber attacks

Practices can take many different avenues to bolster their cybersecurity efforts. One of the most important steps is implementing proper security systems, such as Artificial Intelligence (AI) solutions. These systems are designed to constantly understand patterns and protect data automatically while anticipating and identifying any nefarious activity. In a time where hackers can attack systems in various forms at various times, AI solutions will intuitively protect your network and patient data.

Another step, especially in this remote era of health care, is to have added protection for any mobile devices used by employees. While the amount of mobile devices at our disposal is helpful to radiologists and their practices, they also pose a great threat to network privacy and security. With the pandemic forcing many radiologists and physicians to work remotely, they have relied on their mobile devices and wireless networks at home to accomplish their work. These devices and networks are much less secure than those at their practices, easing the challenge for hackers to attack.

To decrease the possibility of hackings or any unauthorized access, all used mobile devices must be equipped with stronger authentication and access control settings. Regularly changed passwords, further authentication steps and even limiting the amount of mobile devices used are a few ways to increase protection when utilizing mobile devices. Implementing these settings can be a major step in keeping all data and private

information secure as remote work could be the future of the industry, at least for the rest of this pandemic, and maybe even beyond.

Network breachings can be detrimental to practices and their patients in numerous ways. It is important that practices improve, and maybe even overhaul, their cybersecurity efforts. The expansion and evolution of industry technology only increases the chances of network hackings and practices losing invaluable data and information. As many practices struggle to survive during these turbulent times, one network hacking could be the ultimate kiss of death.