WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Increased Threat of Cybercrime in Health Care Industry

Written By **Angela P. Doughty, CIPP/US** (apd@wardandsmith.com) and **Erica B. E. Rogers** (ebrogers@wardandsmith.com)

November 2, 2020

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.S. Department of Health and Human Services (HHS) are aware of an increased cybersecurity threat to hospitals and healthcare providers in the U.S.

This article is to make you aware of this increased threat and provide you with information and resources that can help you avoid, mitigate, and respond to such threats. Our health care and privacy and data security attorneys are also always available to provide additional insight and guidance on best practices for ensuring compliance with any legal obligations arising under such cybersecurity threats.

What Is Malware?

Much like the virus that poses a threat to our personal health this year, "malware," a portmanteau for malicious software, is a computer virus that poses a threat to information security.

The reason malware successfully causes damage to a computer, server, or computer network, is that it is often disguised as harmless. Once it is inside a computer system, it can produce copies of itself and insert them into other computer programs and files. Most malware is designed for the cybercriminal to intentionally steal personally identifiable information, financial information, and other sensitive information. For the healthcare industry, this threat extends to unauthorized access and disclosure of demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual ("Protected Health Information" or "PHI").

What Is Ransomware?

Ransomware is a specific type of malware that disables the victim's access to data until payment is paid. Advanced ransomware encrypts the victim's files, making them inaccessible until a ransom payment is paid to decrypt them. Since the cybercriminals typically demand cryptocurrency, tracing the criminals to prosecute them for ransomware attacks is extremely difficult.

What Can You Do?

There are advanced anti-malware software programs, including on-access or real-time scanners, that can protect computer systems from ransomware attacks. Anti-malware software programs can provide real-time protection and detect and remove malware software that has already been installed onto the computer, server, or computer network.

All health care organizations are encouraged to maintain business continuity plans that will keep them afloat during cyberattacks. Much like wearing masks and washing our hands, healthy strategies for your organization include the following:

- maintain updated systems, software, and firmware;
- encrypt data;
- regularly change passwords and use multi-factor authentication;
- back up data;
- audit user accounts;
- identify critical data assets and create backups offline;
- conduct regular anti-malware scans;
- disable unused remote access;
- monitor remote access;
- implement a cyberattack response plan; and
- implement a data recovery plan.

Also important are employee training programs, designed to inform individuals about the risks of ransomware and how to implement behavior that ensures protection against ransomware attacks. For example, employees should be well aware of how to avoid clicking on malicious links through emails.

More information is available via the AA20-302A Ransomware Activity Targeting the Healthcare and Public Health Sector report recently released by CISA, FBI, and HHS and the Fact Sheet: Ransomware and HIPAA report published by the U.S. Department of Health & Human Services Office for Civil Rights (OCR).

--
For further information regarding the issues described above, please contact Angela P. Doughty, CIPP/US or Erica B. E. Rogers.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.