FBI Warning on Cybercriminals Targeting FTP Servers to Compromise Protected Health Information

By David J. Hochman, Partner

In March 2017, the Federal Bureau of Investigation (FBI) issued a Private Industry Notice (Notice) advising that the FBI is aware that cybercriminals are actively targeting File Transfer Protocol (FTP) servers in "anonymous" mode, which are associated with medical and dental facilities. The purpose of these attacks, according to the FBI, is to gain or steal protected health information (PHI) to use for purposes such as blackmail, identity theft, and/or financial fraud.

File Transfer Protocol, otherwise known as FTP, is used to transfer files between computers on a network (e.g., between a computer account and a desktop or laptop computer or to access online software archives). In this context, the term "anonymous" describes an FTP server that can be accessed with a common username and password (e.g., anonymous), or without a password. FTP servers in anonymous mode are commonly used when the goal is to make information stored on the server readily available, such as through the use of open-source software. While it may seem obvious that placing confidential or sensitive data on an FTP server in anonymous mode is ill-advised, a study done by the University of Michigan in 2015 indicated that as many as 1,000,000 FTP servers were set up to permit anonymous access.

Small medical and dental practices are more vulnerable to this type of attack. In general, small practices do not frequently update their technology and, as a result, they end up with outdated systems that are inadequately secured. Often, an anonymous FTP attack and other types of "silent" attacks are not readily apparent. A firewall will detect if a hacker is attempting to access the server, but will not disclose if a third party is adding dangerous content or changing data on the server. For example, it may be possible for criminals to use an FTP server running in anonymous mode as a drop site for stolen credit card numbers or other illegal activities. Although that does not breach the security of the information on the server, it does permit the FTP server to be used for illegal activities.

In its Notice, the FBI recommended that medical and dental providers have IT personnel check their network for FTP servers running in anonymous mode. If the conclusion is that the practice has a legitimate use for operating an FTP server in anonymous mode, it should ensure that PHI is not stored on that server.

Even if medical and dental practices do not have FTP servers in anonymous mode, they should consider obtaining cybersecurity insurance coverage. The coverage should pay claims based on the unauthorized disclosure of PHI, the failure of computer security to prevent a breach, and regulatory action by a government agency due to the unauthorized disclosure of PHI or a computer breach. In the event of a covered breach, the policy also should provide patients with up to 12 months of free credit or identity monitoring. Some medical malpractice insurance policies offer cybersecurity coverage without additional cost. However, the basic limits on amounts paid under such policies may not be adequate to cover a large breach, particularly when it is not possible to determine which records may have been accessed or copied. For example, in May 2016, a 13-provider family practice and obstetrics/gynecology practice in Texas had its computer system hacked, and potentially up to 68,000 medical records and

personnel files may have been improperly accessed. The practice is reportedly providing a year of credit monitoring to all patients whose records may have been accessed.

The challenges presented to medical and dental practices in safeguarding health care information are not going to disappear, and the methods available to those seeking to improperly access this information keep expanding. For these reasons, health care entities should be proactive and take steps to ensure that the integrity of their computer systems is maintained. While no practice can predict the next type of security risk, each should make cybersecurity a routine priority.

If you would like to discuss your security risks and mitigation efforts, please contact any of the listed attorneys for more information on how Roetzel can help.

Author
David Hochman
dhochman@ralaw.com

Additional Contacts
Ericka L. Adler
eadler@ralaw.com

Mazen Asbahi
masbahi@ralaw.com

Avery Delott
adelott@ralaw.com

Christina M. Kuta
ckuta@ralaw.com

Media Contacts
Wendy Castorena
wcastorena@ralaw.com

Ashley McCool
amccool@ralaw.com