Published on *The National Law Review* https://natlawreview.com

New FBI Warning for Healthcare Providers: Cybersecurity

Article By:

Privacy & Security Practice Group at Mintz Levin

The ***FBI*** has issued new guidance specifically applicable to medical and dental facilities regarding the cybersecurity risk of ***File Transfer Protocol ("FTP")*** servers operating in "anonymous" mode. FTPs are routinely used to transfer information between network hosts. As further described in the guidance, when an FTP server can be configured to permit anonymous users (through the use of a common user name like "anonymous" and without the use of a password) to gain access to the information stored on the server, which might include sensitive information about patients. In addition to potentially directly compromising the security of the stored information, a hacker could use the FTP server in anonymous mode to launch a cyber attack on the entity.

The FBI provides the following specific guidance, which Covered Entities and Business Associates should heed:

> The FBI recommends medical and dental healthcare entities request their respective IT services personnel to check networks for FTP servers running in anonymous mode. If businesses have a legitimate use for operating a FTP server in anonymous mode, administrators should ensure sensitive PHI [Protected Health Information] or PII [Personally Identifiable Information] is not stored on the server.

Coupled with recent advice from FBI Director James B. Comey on ransomware, which we blogged about here, this latest guidance from the FBI demonstrates the seriousness the potential cybersecurity threats facing healthcare entities.

National Law Review, Volume VII, Number 88

Source URL:https://natlawreview.com/article/new-fbi-warning-healthcare-providers-cybersecurity