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

Hackers Demand Ransom to Keep Medical Records Private

Article By:

Privacy & Security Practice Group at Mintz Levin

Medical-data blackmail is becoming more common as more health care providers adopt electronic health records systems and store patient data digitally. This Bloomberg technology blog story describes some of the larger incidents where medical data has been held for ransom by hackers or even unpaid, disgruntled subcontractors.

In particular, the story provides the details of a recent breach of a small Libertyville, Illinois medical practice's server by bold hackers who gained access to patient data contained in stored emails and electronic medical records. The hackers encrypted and password-protected the files they accessed, and then posted a ransom note on the server demanding payment from the medical practice in exchange for the password to unlock the encrypted files. Rather than comply with the ransom demand, the small medical practice shut down the compromised server and called police.

Although storing patient data electronically has its benefits, it is important that medical practices remember that merely storing the data electronically is insufficient to protect the patient from potential identity theft or to comply with federal and, in many instances, state data security obligations. And one-time encryption is never enough. Hackers spend an inordinate amount of time searching for ways to circumvent security measures to access personal data with high monetary value, such as Social Security numbers and credit card numbers.

So what can be done to protect against such threats? While each medical practice should specifically tailor its information security plan to address the unique threats and vulnerabilities it confronts, practices should consider employing several strategies to reduce the risk of authorized persons gaining access to health records systems:

- Install the latest updates and security patches for antivirus and anti-intrusion solutions, and, to the extent possible, encrypt patient data maintained by the practice (whether stored centrally on a server, or locally on a desktop PC, smart phone, tablet PC, or thumb drive).
- Conduct regular backups of patient data to secure storage media. The practice can retrieve and use the backup patient data should locally stored data be lost or stolen.
- Develop and enforce comprehensive user access policies that are applicable to all employees and third-party contractors (including business associates and business associate subcontractors). These policies should identify those individuals or classes of individuals who are authorized to access and/or modify patient data; manage the means by which such individuals can access patient data (e.g., directly through an in-office workstation, remotely

via a smart phone or tablet PC, etc.); as well as describe the procedures for activating and terminating user access to patient record.
- Assign each authorized user a unique user ID, which the practice can use to properly monitor and track user activity as well as assign appropriate credentials to control access to sensitive data.
- Disable or strictly limit the use of administrator IDs for electronic systems containing patient data.
- Employ auditing software that can alert practice management to potential security incidents and inappropriate data access in near real time.

The list above is illustrative only and provides no substitute for a thorough risk assessment and comprehensive information security plan. The ease by which practitioners can electronically access and modify patient records is also the greatest weakness. However, sound security practices and solutions can help mitigate the financial and legal risks if appropriately employed and configured.

National Law Review, Volume II, Number 238