# Cyber-Security in the Age of Ransomware
## By: Frank Sivilli

Cybersecurity is becoming increasingly important for running a business in healthcare. The risk of data breaches and data loss should be a core motivation behind any preventative initiatives you undertake to protect your business.

**Encryption** is a means of securing data by converting the information into an unreadable piece of code. The encrypted data can only be accessed by use of a matching digital key. Encryption is one of the most effective ways of securing data in any business, but especially in a health care setting.

According to Forbes, health care data is worth three times as much as financial information on the dark web. For that reason alone, health care data is becoming a primary target for cyber-attacks.

The **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** sets security standards that apply to health care providers around the country regarding the proper use encryption that must be in place to protect patients' sensitive health care data. Under HIPAA, particular standards must be in place to address the privacy and security of protected health information (PHI). **PHI** is any demographic information that can be used to identify a patient. HIPAA regulation lists 18 identifiers that are considered PHI, some of which include a patient's name, address, phone number, Social Security number, insurance ID number, medical record, or full facial photo, to name a few. PHI stored, maintained, transmitted or handled in a digital format is called electronic protected health information (ePHI).

**What is Ransomware?**

**Ransomware** is a type of malicious software that infects computer systems and encrypts data being stored on the network or computer. The data is then made inaccessible to anyone but the hacker. The affected practice is left unable to access their data--and to make it worse, the hacker

often demands a sum of money to be paid by a certain date, or else risk permanently losing access to the data.

The practice of essentially ransoming off health care data has become pervasive, affecting health care providers large and small. In May of 2017, one of the largest ransomware incidents on record shut down most of the UK's National Health Services and affected the health care systems and governments of over 15 countries around the world.

In a health care setting, ransomware affecting unencrypted ePHI is almost always considered a HIPAA violation. If the data is unencrypted, that means that hackers who have perpetrated a ransomware incident can potentially gain access to it, compromising patient privacy and data security.

HIPAA guidance from the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) states that health care organizations that have experienced a data breach should contact local law enforcement to help investigate and track the incident.

Even if the ransom is paid, there is no guarantee that access to the encrypted data will be restored or any assurance that the hackers have not already accessed it.

**HIPAA Security Rule Requirements**

The HIPAA Security Rule sets specific standards for maintaining the confidentiality, integrity, and availability of PHI. These standards are broken down into three categories of safeguards, which include:

- **Technical Safeguards:** These include any and all cyber-security protections that health care professionals must have in place to protect ePHI. Some examples of technical safeguards include firewalls, encryption, anti-virus/anti-malware protection and secure communications.

- **Physical Safeguards:** These include security measures taken to secure the physical premises where PHI or ePHI is maintained. Common examples include locks on doors, alarm systems, key-card access, locked shredding bins and locked server rooms.
- **Administrative Safeguards:** These include different means of ensuring that members of the workforce are adhering to and helping to reinforce security safeguards. Examples include policies, procedures, annual HIPAA employee training and quarterly cyber-security awareness training.

**HIPAA Encryption Specifications**

HIPAA regulation identifies two types of data, each of them with specific encryption specifications that must be addressed to safeguard ePHI.

**Data at Rest** is any information that is stored on a server, hard drive or computer system that is not being actively transferred or transmitted while it is being maintained.

**Full Disc Encryption** is a means of encryption that helps you protect data at rest. By implementing full disc encryption, you are protecting an entire hard drive or server, rather than individual files containing ePHI. Full disc encryption provides a far more advanced level of security and is one of the only effective ways of ensuring that ePHI cannot be accessed in the event of a ransomware incident.

**Data in Motion** is any information that is being electronically transferred or transmitted.

**End to End Encryption** (E2E encryption) is a type of encryption that can help protect data in motion. E2E encryption helps ensure that any data that is being transferred is only viewable by the party sending the information and the intended recipient. It's important to realize that ePHI that is sent via non-encrypted email or communication medium is not secure. That's because when information is sent via email, for instance, that email is stored on an email provider's servers.

While that ePHI is stored on the server, it is potentially viewable by the email provider or any hackers who may have gained access to that provider's servers. E2E encryption prevents this type of inappropriate access to ePHI.

**Off-site data backup** is another effective means of securing data in the event of a ransomware incident. Off-site backup is a type of data backup that essentially creates a direct copy of all of your data and stores it on a third-party server that is housed in a different physical location. Routine data backup ensures that updated copies of data are kept in a secure, third-party location that can be accessed at any time. Off-site data backup also ensures that the same ransomware strain will not spread to the copies of the data being maintained off-site. This is important because off-site backup gives providers the ability to restore access to affected data almost immediately, in the event of a ransomware incident where ePHI has been maliciously encrypted. While this does not erase the potential impact of a ransomware incident or data breach, it does allow for regular business operations and patient care to resume.