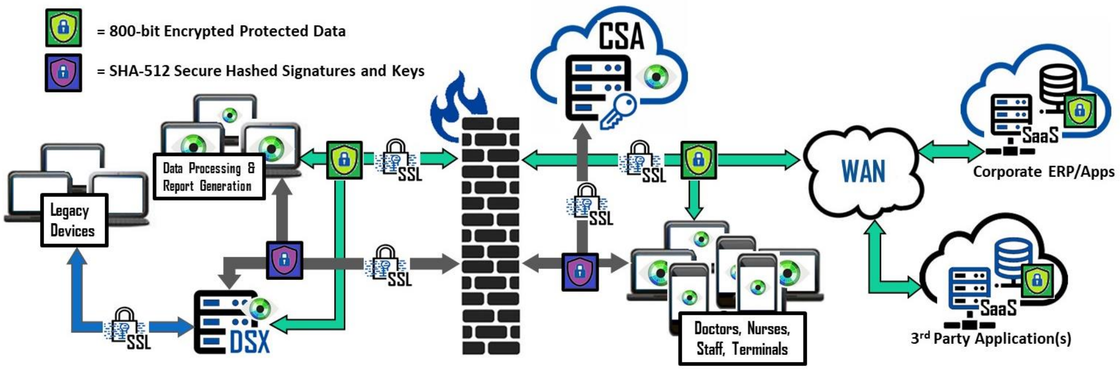
Use Case: Protected Health Information under HIPAA

Enacted in 1996 by the Department of Health and Human Services ("HHS"), the Privacy Rule regulates the use and disclosure of protected health information (PHI) by the Healthcare industry.

Healthcare is a lucrative target for cybercriminals who exploit misconfigured IT infrastructure and applications by using attacks such as weaponized ransomware and phishing emails. In the last 10 years, cybercriminals successfully accomplished and often monetized 2,181 healthcare data breaches. Those breaches resulted in the theft/exposure of 176,709,305 healthcare records - equal to nearly half the population of the United States. Healthcare data breaches are now reported at a rate of more than one per day. The largest in 2018, UnityPoint Health notified 1.4 million patients their records may have been breached when its business system was infiltrated. Sadly, this was the second breach for UnityPoint where phishing attacks at their Madison campus breached the data of 16,000 patients five months earlier. In all cases, the problem arises from the common practice of creating concentric layers of security as an attempt to keep attackers out rather than using a data-defined protection approach to directly protect the data.

On the other side of the coin are internal threats. Breaches are often attributable to the use of personal mobile devices in the workplace. BYOD policies have created new vulnerabilities in which up to 80% of healthcare providers use smartphones, tablets, or laptops to support their workflows. According to a survey conducted by Health Information Trust Alliance, 41 percent of PHI breaches are attributable to the theft of an employee´s mobile device or portable media.

Deploying Bonafeyed's technology in Healthcare database backed applications, encrypts patients' PHI in real-time and the data remains protected when accessed by authorized staff, accountants, physicians, or registered nurses at terminals or on mobile devices. In addition, patient data placed in backend ERP systems, shared in the cloud, or archived remains protected.


= 800-bit Encrypted Protected Data
= SHA-512 Secure Hashed Signatures and Keys
CSA
Data Processing & Report Generation
Legacy Devices
SSL
SSL
SSL
SSL
SSL
DSX
WAN
SaaS
Corporate ERP/Apps
SaaS
3rd Party Application(s)
Doctors, Nurses, Staff, Terminals

Furthermore, the Bona-Data™ Enterprise Gateway (DSX) facilitates the fastest deployment option for legacy devices or applications without the need for endpoint plugins or altering applications. Bonafeyed can individually protect PHI data fields within ERP backed databases and with Bonafeyed's Cy4Secure Arbiter (CSA), it validates and authorizes access to protected data using an 800-bit Stream Cipher or AES256 encryption technologies.

A lost or stolen, unencrypted or non-password protected device is the number one HIPAA violation. When a Bonafeyed data encrypted device is taken, abandoned, or forgotten, its data remains protected, inaccessible and demonetized. Deleting its keys ensures cybercriminals or internal non-authorized users obtain no data, which exceeds ***HIPAA's data privacy rule!***

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.