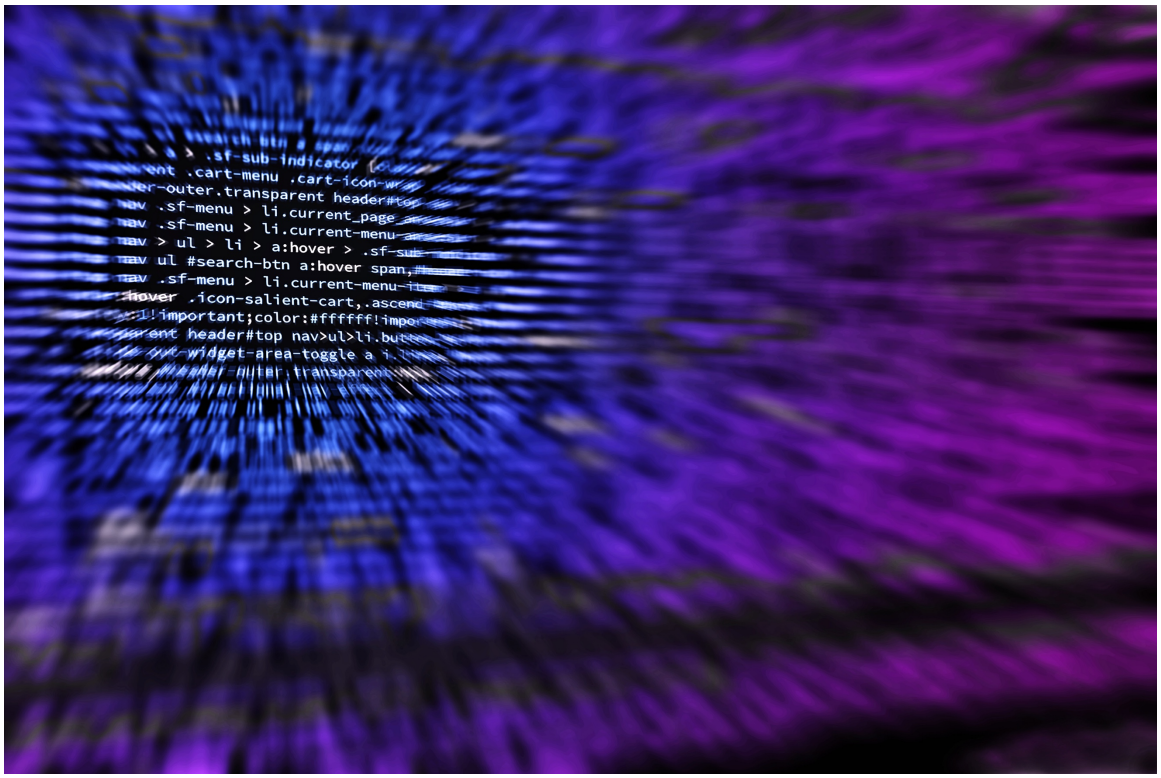
UNENCRYPTED

Protecting Healthcare Data Against Cyber Attacks

November 2017

Table of Contents



Introduction

It should come as no surprise to professionals that data breaches and security hacks are a concern for businesses across the world. But, it may be surprising to learn that a Raytheon study found that 97% of networks will experience a security compromise over any six-month period.[1] That means that businesses of all sizes, professions, locations, and structure are prime candidates for a cybersecurity attack—including, in particular—healthcare organizations.

In 2017, more than 3.1 million Americans' healthcare data was compromised due to data breaches, and that number is expected to increase exponentially with time.[2] The biggest threats to cybersecurity across all professions? Weak, default, or stolen password.[3] The biggest threat in healthcare? Hackers and insiders.[4] In fact, the 2017 Protenus Breach Barometer report found that 41% of examined data breaches were a result of insider error or wrongdoing, and hacking was to blame for more than 32% of data breaches.[5] When it comes to protecting millions of patient records and ensuring best business practices, the health care sector has just one unequivocal solution: full database encryption.

[1] http://assets.theitjobboard.com/ITMEDIA/default/Taylor/Raytheon/DataClarityInvestigativeAnalyticsWP_FINAL.pdf
[2] http://www.fiercehealthcare.com/privacy-security/healthcare-data-breaches-haven-t-slowed-down-2017-and-insiders-are-mostly-to-blame
[3] http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf
[4] http://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches
[5] http://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches

The Unique Case of Health Care

Health care is a prime target for security breaches because of two critical factors: highly valuable patient information and steep liability. In 2016, there were at least 377 known healthcare data breaches, and more than 87% of healthcare lawyers believe that healthcare organizations are at a greater risk of cybersecurity attacks than other industries.[6] In addition, healthcare data breaches cost more to rectify than breaches in any other industry, coming in at an average of more than $400 per patient record.[7]

Risk factor: Patient Data

Patient data is ripe with profitable information. A typical patient file, including medical records and payment information, will include a litany of data points that any hacker would love to obtain. Personal information, like age, address, and Social Security number, is easily sold to willing buyers who want to steal identification. Financial records include insurance information and claims reports, which are often used for filing fraudulent claims in an effort to collect payouts. And, of course, there's patient health information, which can be sold on the black market for 10 to 20 times the amount of cash as personal information. Stolen patient data enables a hacker to order and resell expensive drugs, commit medical identity theft, and more.[8]

[6] http://www.modernhealthcare.com/article/20170121/MAGAZINE/301219987
[7] https://www.calyptix.com/hipaa/healthcare-data-breaches-expensive-average/
[8] https://www.popsci.com/why-do-hackers-want-your-health-data

Risk factor: Liability

Because of the vulnerabilities of protected health information (PHI), the Federal government vowed to hold healthcare providers liable for lost or compromised patient data under the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules. Designed to protect the privacy and security of individuals, health providers are deemed responsible for properly securing and protecting patient information. The red flag for medical providers appears when it comes to identifying the entity held liable for data breaches of this type of information, as the HIPAA Privacy, Security, and Breach Notification Rules explicitly state that the rules apply to all HIPAA-covered entities *including business associates*.[9]

This seemingly innocuous information is critical for health care organizations to know and understand. In short, providers are held responsible for data breaches *even if their vendor is responsible for the breach*.[10] Third-party vendors like billing services, legal entities, payment processing companies, and health management information systems can all be the sources of a data breach for which the provider organization is held responsible.

Risk factor: More employees

Many small- and medium-size healthcare organizations feel that they are the underdog in the battle of fighting security attacks. Limited budgets make high-dollar malware detection software or fulltime staff dedicated to security unrealistic. While this argument may seem practical at its core, the data and research tell a different story.

Smaller medical groups are not necessarily more likely to be impacted because of lower prevention budgets. In fact, a 2017 study reported that larger hospitals and teaching-focused facilities can create higher data breach risk—a result of increased exposure at the individual level.[11] As more and more people are given access to patient data, potential sources for a breach increase simultaneously.[12] These sources include stolen credentials, lost devices like cell phones or laptops, simple mistakes, or security ignorance.[13] In short, hackers go where the money goes—so larger organizations have more patient records and more points of access, making larger organizations more likely and easier targets for attacks.

[9] https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf
[10] https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf
[11] https://healthitsecurity.com/news/healthcare-data-breach-risk-higher-in-larger-facilities
[12] http://www.healthcareitnews.com/news/healthcares-worst-security-weakness
[13] https://www.cio.com/article/3078572/security/human-error-biggest-risk-to-health-it.html

Risk factor: Outsourced Services

The healthcare industry is also seeing an increased number of providers using foreign software vendors and billing services. Although offshoring is not illegal, it poses particular risks to healthcare organizations, particularly in the areas of compliance and legal issues. For instance, although a healthcare organization follows HIPAA compliance rules and performs due diligence on its vendors, HIPAA and other United States security laws do not apply and are not enforceable outside of the United States. Furthermore, HIPAA does not directly address all potential privacy and security risks to an organization.[14] In other words, although a medical group and its business entities follow HIPAA compliance and guidelines, it does not remove liability if an offshore IT or support department with access to unencrypted data is breached.

Additionally, offshore vendors are not held to the same safeguards and reporting requirements that are required within the United States, meaning a healthcare organization may not actively know about a security breach that occurred in an offshore vendor network, increasing liability if a data breach is later discovered as untimely reported.

Risk factor: Outdated Technology

An assessment of healthcare data hacks revealed that medical organizations are particularly vulnerable to hackers due to the general age and inadequate nature of healthcare technology infrastructure.[15] In comparison to other markets, like banking and retail, technology in the healthcare industry is slow to change, making it much easier to hack.

[14] https://www.healthlawyers.org/find-a-resource/HealthLawHub/Documents/Cybersecurity/Journal_2014_Offshoring%20Health%20Information.pdf
[15] https://www.cio.com/article/2880771/data-breach/what-the-anthem-data-breach-says-about-the-vulnerability-of-healthcare-it.html

Many healthcare practice management software systems were built with old technology that is no longer supported or updated with security updates, meaning it lacks the security features and is more vulnerable to hackers' attacks than new software technologies. After a breach, authorities will assess fines and penalties based on the actions taken (or not taken) by an entity to prevent a data breach. Using old technology software for processing confidential patient data may prove to be very costly if there is a data breach. It is important to note that a data breach does not need to impact a high quantity of patient records to incur enormous fines. For instance, Oregon Health & Science University was fined nearly $3.0 million for breaches that impacted 7,000 records after an older laptop with no encryption software was stolen.[16]

Implications of Data Breaches in the Medical Profession

Businesses are spending more and more every year to recover from a security breach, regardless of industry. From lawyer fees to security updates to technology repairs, the average total cost of a security breach exceeds $3.5 million.[18] In healthcare, that number rises to more than $4 million on average.[19]

The HIPAA Breach Notification Rule requires that covered entities notify all affected individuals, HHS, and, in some cases, the media when a breach is detected. In addition, the Notification Rule requires that the communication must be provided without unreasonable delay and no later than 60 days following the discovery of a breach.[20]

[16] https://www.beckershospitalreview.com/healthcare-information-technology/10-largest-hipaa-settlement-fines.html
[17] https://www.cio.com/article/2880771/data-breach/what-the-anthem-data-breach-says-about-the-vulnerability-of-healthcare-it.html
[18] http://assets.theitjobboard.com/ITMEDIA/default/Taylor/Raytheon/DataClarityInvestigativeAnalyticsWP_FINAL.pdf
[19] http://www.healthcareitnews.com/news/cost-data-breaches-climbs-4-million-healthcare-events-most-expensive-ponemon-finds
[20] https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf

A commissioned 2017 study[21] found that the disclosure of a data breach has a profound impact on a business's reputation, including:

- Average stock devaluation of 5%
- Increased customer turnover of 7%
- Consumer decrease in brand trust of 65%
- More than a 30% loss in consumer relationships

Data breach cost category proportions across 10 years - 2016

Table 2 Cost change	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Investigations and forensics	8%	8%	9%	8%	11%	11%	12%	13%	14%	15%
Audit and consulting services	10%	10%	11%	12%	10%	9%	8%	7%	7%	6%
Outbound contact costs	9%	7%	6%	6%	5%	6%	5%	4%	3%	4%
Inbound contact costs	10%	8%	6%	5%	6%	5%	5%	6%	5%	4%
Public relations/ communications	1%	3%	1%	1%	1%	1%	1%	1%	1%	2%
Legal services - defense	6%	8%	9%	14%	14%	15%	15%	16%	16%	15%
Legal services - compliance	3%	3%	1%	2%	2%	3%	4%	3%	4%	3%
Free or discounted services	2%	1%	2%	1%	1%	1%	1%	2%	1%	0%
Identity protection services	3%	2%	2%	2%	2%	3%	4%	2%	2%	2%
Lost customer business	39%	41%	43%	40%	39%	37%	36%	38%	39%	40%
Customer acquisition cost	8%	9%	9%	9%	9%	9%	9%	8%	8%	9%
Total	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Source: Ponemon 2016 Cost of Data Breach Study: United States

The long-term cost of a data breach may be far more than the sum of the fines, fees and other direct costs; in fact, "In a typical breach, 40% of the cost is due to losing customers. Since healthcare has an even higher rate of churn, this pushes its cost-per-record through the roof."[22]

[21] https://www.centrify.com/about-us/news/press-releases/2017/ponemon-data-breach-brand-impact/
[22] https://www.calyptix.com/hipaa/healthcare-data-breaches-expensive-average/

Methods of Security Protection

Encryption

One of the core methods of protecting private information and patient data is through encryption. Properly encrypted data deters hackers, as it offers only scrambled text and information with no decipherable decryption code. Encryption uses an algorithm to turn plain text, like letters and numbers, into an unreadable code. To unscramble the information, an encryption key is required.

Encrypting data requires extra processor power and consumes more storage space. Prior to HIPAA, the protection of data was viewed as less important than pure accessibility.[23] Most of the largest practice management and billing systems in the industry today were designed and built before HIPAA and, as a result, they store confidential data as unencrypted. Even most new practice management and billing systems continue to store confidential data as unencrypted because while it is recommended by HIPAA, it is not required by HIPAA. Encryption adds complexity to the development process, consumes resources, and the benefit is not directly visible to the end user.[24]

While there may be no 'visible' benefit to the end user, encryption is the only method that can protect a health care organization from a data breach.

The Need for Ongoing Encryption

Encryption offers healthcare organizations a method of data and company protection by removing the 'confidential' status of the data. According to HIPAA guidelines, data that has been encrypted is no longer confidential, and therefore not subject to breach reporting requirements. That is, if an unauthorized person only has access to encrypted data at the time of a security breach, a covered entity does not need to report the data as a data breach.

The National Institute of Standards and Technology, which is part of the U.S. Department of Commerce, issued a special publication, *Guide to Storage Encryption Technologies for End User Devices*, to help organizations mitigate their risk and exposure in storing data. The recommendations outline the various forms of encryption and technologies as well as the laws and regulations that define the need for proper storage and security.

One notable exclusion from the recommendation is the lack of requirement to encrypt sensitive data *except when in transport*. As a result, most software solutions available to medical groups encrypt data while in transport but the data is unencrypted while at rest in the database, thus exposing sensitive information to anyone with access to the database.

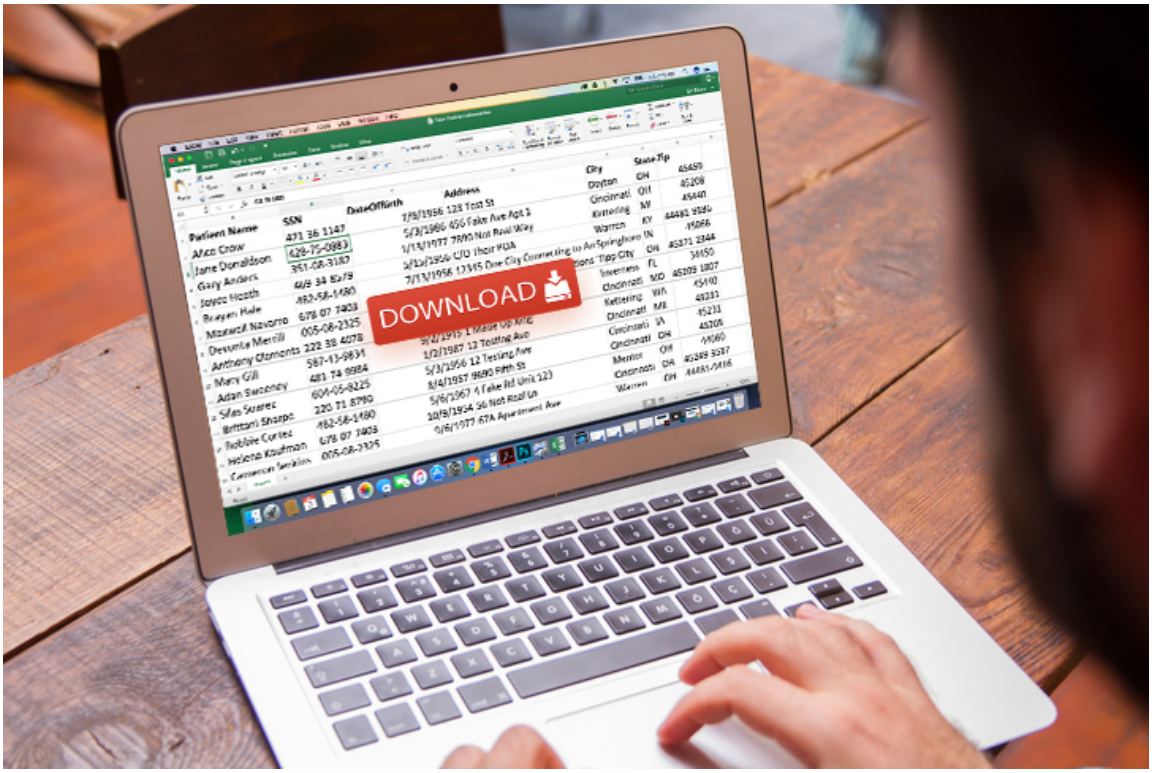
[23] http://www.techrepublic.com/blog/tech-decision-maker/life-before-hipaa/
[24] https://www.winmagic.com/blog/2016/09/27/encryption-challenges-changing-tech-world/

Even if the database is stored on an encrypted drive, the data is plainly visible to someone with authorized access to the drive. This exposure is where all medical organizations and practices should identify a red flag: When data is at rest, it is at risk.

The 'Always Encrypted' Problem

SQL Server attempted to address this weakness by offering enterprises an 'Always Encrypted' feature in its 2016 release. The feature offered a system for encrypting data at rest and during transport; however, analysts quickly noted the product's "many limitations," including restrictions to encryption services and the complexity of implementation.[25]

Solutions like SQL Server and encrypted drives appear, on the surface, to tackle the problem of protecting data at rest. The truth is that access to unencrypted data is simply a matter of obtaining authorized credentials—a cornerstone of any hacker's approach to getting private information. With the right login information, the data is unencrypted and available to anyone using the authorized credentials, including a hacker.



[25] https://www.red-gate.com/simple-talk/sql/database-administration/sql-server-encryption-always-encrypted/

Recommendations & Solutions

The first step to protecting your medical group is identifying the tools, policies, and procedures your organization needs to comprehensively protect your data. With the increased complexity of hacking, the healthcare industry continues to be a prime target for security breaches.

In almost all solutions offered to the healthcare community, data breach protection for the database that stores confidential patient information comes down to protecting the user credentials of authorized users who can view the confidential data as unencrypted data. Hackers have proven to be very resourceful and very successful at stealing these credentials time and time again despite a medical group's best efforts to secure the information.

There is one innovative practice management software company with a practice management software that has closed that door to hackers and made its database virtually breach proof. They do this by encrypting all data from the time it is entered, during transport, and as stored in the database as encrypted. No one, regardless of credentials, can view the data in the database as unencrypted. That practice management software is ProSourceMD, a state-of-the-art software used by medical groups and billing services for anesthesia and general medical billing.

Solution: ProSourceMD

ProSourceMD, a product of Navaro Medical Solutions, may be the only practice management software available on the market that stores all confidential data as encrypted data *during transport and in the database while at rest where no one can view the confidential data in its unencrypted state*. Since encrypted data is not considered confidential data, it makes ProSourceMD database breach-proof.

ProSourceMD was designed from the ground up with state-of-the-art technology to exceed the privacy and security features recommended by HIPAA, going well beyond the minimum requirements in many areas. When data is encrypted with ProSourceMD software, it remains encrypted—even when retrieved by the program. The decryption only occurs in the application when it needs to be displayed to a validated and authorized user. In most cases, only a single individual's information is being viewed unencrypted at any given point in time.

No single person or program can ever view or export data from the database as unencrypted. This differentiator is critical. Unlike most available software programs, which leave data vulnerable to anyone with an authorized login, ProSourceMD ensures that no user can access original, unencrypted data in its database. ProSourceMD stores encryption keys offsite, fully separate from the software and database. In addition, ProSourceMD uses AES256 encryption and goes an extra step to fully obfuscate the encryption and decryption process, thus making it impossible to decrypt the data, even if a hacker were able to steal the database and encryption keys.

Using ProSourceMD for your billing software or using a billing service that uses ProSourceMD gives medical groups a level of protection they cannot get through any other software, or through any amount of insurance or through any amount of network safeguards. If you can prevent a data breach that could cost you millions of dollars and ruin your practice's reputation, why wouldn't you?

Below is an image of unencrypted data as it typically appears to those with database access:

PatientName	SSN	DateOfBirth	Address	Phone	InsuranceID
April Koch	947-07-9004	1960-04-06 00:0...	65 East Green N...	8482812010	497430358
Lora Salinas	903-67-7022	1966-06-25 00:0...	81 Cowley Blvd.	980-4970581	365548782
Felicia Simpson	944-14-7376	1961-10-16 00:0...	46 Nobel Way	976-9412266	210417541
Darnell Espinoza	638-45-3700	2003-06-11 00:0...	56 East White H...	4228999693	675488026
Grant Clay	463-87-6172	1986-03-09 00:0...	678 Rocky Seco...	6094495752	831917171
Bruce Johns	377-76-2471	2002-02-13 00:0...	39 Nobel Freew...	231-830-9888	538792932
Grace Garner	902-79-8315	1965-10-20 00:0...	74 Green Secon...	257220-0321	593505106
Robbie Mc Intyre	168-19-8138	1973-01-14 00:0...	822 West White...	046556-2952	852158002
Alvin Hall	796-28-7507	1956-03-31 00:0...	18 North White ...	660996-9292	573973874
Wendi Dickson	419-63-2124	1975-11-14 00:0...	645 Rocky Cowl...	418-5287939	869059059
Owen Gillespie	821-22-6267	1994-10-27 00:0...	838 Cowley Road	2683230763	610440172
Cristina Levine	206-38-1800	1965-01-06 00:0...	12 Clarendon St.	3530144742	281907548
Norman Soto	022-16-4552	2001-10-03 00:0...	32 Old Road	066-2322718	745181516
Garrett Noble	735-91-8319	1977-06-03 00:0...	771 Green Cowl...	755-1570298	851674785
Brett Terry	768-33-7114	1993-08-19 00:0...	740 Hague Ave...	681-4050360	114329500

In comparison, below is an image of encrypted data from ProSourceMD. Note: **This is the only way data ever appears to those with database access in ProSourceMD.**

PatientName	SSN	DateOfBirth	Address	Phone	InsuranceId
1Y6Xk5QamSxYt5eBr...	!qMtyzBVI7gDN/MvH...	!UvE5OulrFnyCOnXYd8OLBcW...	!zz9TY0oQxUQ2WmoPlzcXg==	!1R enuiLIL6soP/xicaavU...	!nM9QB.IyKaqCUJjAKG15..
!Y9{k5QamSxYt5eBr...	!qMtyzBVI7gDN/MvH...	!UvE5OulrFnyCOnXYd8OLBcW...	!zz9TY0oQxUQ2WmoPlzcXg==	HRenuiIL6soP/xicaavU...	IRN6T5Igft6F8wV+E+k9..
!akYML+LDOBaB549...	HUXixuYmDvJbxyPV...	!BM exRqL3ImvqwWo7GmBG...	Z7lbzsjyUNO0eCCI<XBrrq8mrs5L...	ZVECiD7dMAVA5LaNH5...	Zw6xdz4D0sOuy1ny93V..
!j25wf+hK59KG/Jp4q...	!QXPgKNSiCgCsS27...	IhYW3LHENqU5Lecialzq2Bp...	ZhtAzt7j1mDYtzV2zYd+JvLX5+0...	ZNxikCaFBx9InhIXiexvYZ7	ZeaswOlf+uaTzT0F8v6rc..
!j25wf+hK59KG/Jp4q...	!QXPgKNSiCgCsS27...	!hYvvi3LHENqU5Lecialzq2Bp...	ZhtAzt7j1mDYtzV2zYd+JvLX5+0...	ZNxikCafBx9InhNiexvYZ7...	ZW/wPkTc9GrFDBFDIA...
!tb/DMkxV5B2CINkR...	!Pa4JScBXTd5GEbz...	!rY5vNCF4zqsDHguXc5{63iNpf...	!uf/ZuGP2jw8yJ42>O<MrJgc0w6r...	!epxvyuU+AXVOE/Q0vc...	!MrDFJ8dS1YIL4gMnCbY.
!tb/DMkxV5B2CINkR...	!Pa4JScBXTd5GEbz...	!rY5vNCF4zqsDHguXc5{63iNpf...	!uf/ZuGP2jw8yJ42>O<MrJgc0w6r...	!epxvyuU+45tV0E/Q0vc...	!Pa2h2psnxcaAvHy+kOh...
!FI6YNiOhDORtVagin...	!QlieN/gdim85o0Nj3...	!rWOhcLxrcRQ8KEKYGCiOVhV...	!fNa8XDMW+IF78viTyYeXtoDLy...	!JPXknesW7BVytWsZPIL...	!gSPAcPPOCJ/UF9g/917..
!/UFVPx9IqH7RV88E...	1511v1r50dTaW6GuleL...	GdJoN2tU0aa666wnw7ykK...	!yt0Q4IN5Cb3s8bDxxxR0lpvm1P...	!n+InocySpLPOFEG+8TzS...	!hKtwQbPGUrWLB54+4...
!/UFVPx9IqH7RV88E...	15rMr50dTaW6GuleL...	GdJoN2tU0aa666wnw7ykK...	!yt0Q4IN5Cb3s8bDxxxR0lpvm1P...	!n+InocySpLPOFEG+8TzS...	!hKtwQ13PGUrWLB54+4...
!/UFVPx9IqH7RV88E...	151M150dTaW6GuleL...	GdloN2tU0aa666wnw7ykK...	DELIm1X5MqQ+/hDVMBEdiviQ...	!n+InocySpLPOFEG+8T2S...	!hKtwQ13PGUrWLB54+4...
!/UFVPx9IqH7RV88E...	151M150dTaW6GuleL...	GdJoN2tU0a3666wnw7ykK...	DELIm1X5MqQ+/hDVMBEdivia..	!n+InocySpLPOFEG+8TzS...	!hKtwQ13PGUrWLB54+4...
!bAPYwrVIT22rJ4EB...	!bmuDtbjpxu0Fzo6ck...	!fo37grD4RdByKrw1V2XJ5y8fPv...	!CuSMSOSI6Dr9/4pBo61yPNmK...	!PqzpouYDaCDIiNvoqEtL...	!RtUObyvWOA6ykBYvyH..
!2kORrJuxCHrbkrv1J...	!N/zpUXZrOvQuBQIH...	!JCOtSBCY5EFTbVigDqtUEmsB...	ZG6KWjUWCCYNr0Q76DFx+Xs...	ZUB3DzaCrIO+sIcGQ96C...	ZQctMrs/QdPC98Dc9PX..
!7g1s0tmAcaEcn2OH...	153yk5HRnpm.IF8f1JB...	bliptRZubLRLDTjb+MWNVwZ...	!3WAQ51UBLq4i4PlbysNqLg==	!+2y/N8pN4htBuw3h9BM...	!PUownmCc8X7GdRe9L...
!yub1RyFb010AlaW...	!030u3+PLFoQqsREi...	!pLe/62mM18YBRI8TduYnT9...	Zo+9+bQ6GaMP+4V4GKptBZw...	ZR7/4Pes/hthtChBQ+2JA...	Zp/481grB+cqMvUl3Sw...
19W2dZc4331usza5e...	RuC8i0PDZghcNTZ...	!WPRW7dGYmHTx3uESNhj7S...	Zigfg15MDk4uVQKT5qd//JJQtH...	Z2zDm/gepfGyjwmUWoA...	ZJKhuke4FQunSLFxoM8..
!pt1 v1 jUljrwFFOFuL8...	Hp270BfuH9jCYs3M/...	!nphoQ9sLI/tDr6kMaPNBVIDj2...	!ZmdD6WyvfpvuqIf9gmDBjg==	!PjrL9f4eoe8X4Wjh3IL34...	UrTMDjSjDgFg1CUuE111...

Third-Party Verification: John Parmigiani

Navaro Medical Solutions contacted expert John Parmigiani, an independent information systems technology consultant, to perform a HIPAA Security Rule compliance assessment of ProSourceMD. In his 35-year career as a former federal executive in health information management, Parmigiani served as the federal government chairperson for the interdisciplinary team that developed the HIPAA Security Rule and is well respected as an expert in the field.

Upon completion of the assessment, Parmigiani wrote:

> A distinguishing security feature of ProSourceMD is its encryption of sensitive data at all steps in the process, assuring protection from both internal and external unauthorized access and exposure while mitigating and minimizing client risks. ProSourceMD encrypts data from its inception, when being captured, immediately encrypts it in storage, and provides the capability of sending it securely to any carrier that is equipped to accept electronic transmissions. This process greatly minimizes any potential data loss or corruption threats that result from needing to transmit from provider (the medical practice) to the insurance carrier. Of special importance is the fact that NMS in its ProSourceMD System stores the data in encrypted format, making it virtually impossible for unauthorized access. It is this attribute which makes ProSourceMD consistent with even the most stringent state data protection requirements. **It is safe to say that ProSourceMD stands alone as an E-Health ready practice management system.**

Conclusion

The healthcare industry is in a new era of data security. With breaches on the rise and hackers developing more complex and debilitating ploys, ensuring data protection is no longer a luxury for big-budget providers alone. There are regulations in place and rules to follow. Businesses are required to assess their vendors and partners, including those offshore, to ensure that they are doing everything they reasonably can to prevent confidential data from being compromised. Unfortunately, best efforts do not count for much: if there is a data breach, the healthcare group will pay. When it comes to the question of whether to use software that makes your business breach-proof, the answer is simple: can you afford not to?

Organizations across the field must pay attention to what history is telling us: your business is going to be implicated in a breach. With more than 93% of businesses falling into the 'victim' category, the only way forward is to find fail-safe solutions that protect your data, your business, and your company's future.

About Navaro Medical Solutions

Navaro Medical Solutions has been specializing in developing anesthesia billing software supporting anesthesia groups and multi-specialty billing services for more than 25 years. ProSourceMD, the company's newest software, is a best-in-class anesthesia and general medical billing software program. ProSourceMD was designed and built around the HIPAA regulations using state-of-the-art technology and employing industry-leading security features that make its database breach proof. To learn more about Navaro Medical Solutions, visit www.prosourcemd.com or call (859) 586-0300.