Role of Emerging Technology in Securing Rural Healthcare

Sneha Mirajkar **Vittalkumar Mirajkar**
SMirajka@cisco.com Vittalkumar_Mirajkar@mcafee.com

Abstract

“With great power comes great responsibility”. As the rural healthcare moves towards digital transformation, adopting new and emerging technologies fast pacing the need to cater patient needs and increase the reach to wider population.

In steps, the greatest need for data security or “Patient Data Security” in rural healthcare. Especially, when the need for digitization of rural healthcare is a necessity owing to the pandemic in the recent years. Community and rural hospitals face many challenges in effective communication. Patients might have limited access to healthcare portals or apps. Providers may find it hard to stay in alignment with individual patient needs. Streamlining clinical collaboration is critical to maintaining quality of care while demand increases. Deploying secure messaging platforms enables easy provider-to-provider, provider-to-nurse and system-to-patient communication over voice, video or text.

The primary focus of this paper is to present an overview of the security gaps in the process of digitization of rural healthcare and to highlight the role of emerging technologies in securing the rural healthcare system ensuring Patient Data Security while providing seamless transformation. As the healthcare cybersecurity landscape grows and new threats emerge, healthcare IT professionals must balance IT security policy, processes, and compliance with the need to maintain seamless data flow and timely access to patient information.

Biography

Sneha Mirajkar is a Senior Software Engineer at Cisco, with 14+ years of experience in software testing and extensive hands-on in test automation using Python, AWS, web-services. She has expertise in AWS applications.

Vitalkumar Mirajkar is a Senior Engineering Manager at McAfee, with 16+ years of testing experience ranging from device driver testing, application testing and server testing. He specializes in testing security products. His area of interest is performance testing, soak testing, data analysis and exploratory testing.

1. Introduction

With more sophisticated cyber-threats against healthcare organizations on the rise, having a comprehensive solution in place is critical. The right measures can protect sensitive patient data and prevent security breaches from interfering with patient care.
How far would you go to protect your patients' sensitive data? One thing is for sure — you'll need to stay ahead of the cybercriminals. The topic of healthcare data security has recently come up in the media on multiple occasions, mostly in connection with breaches and leaks.

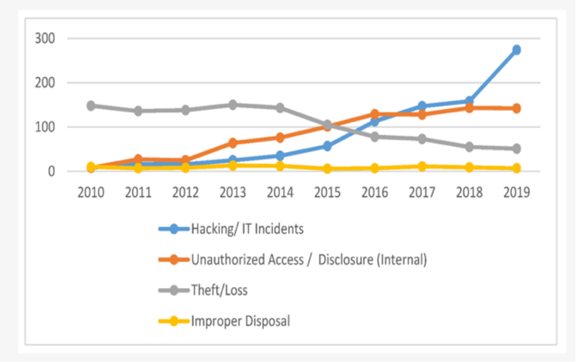
Digital methods as mentioned below; are important to improve the quality, safety, effectiveness, and delivery of healthcare services in rural communities. Connecting rural patients and providers in remote locations to specialists in urban areas. Implementing, maintaining, updating, and optimizing the same can be an ongoing challenge for rural facilities and providers with limited resources and expertise.

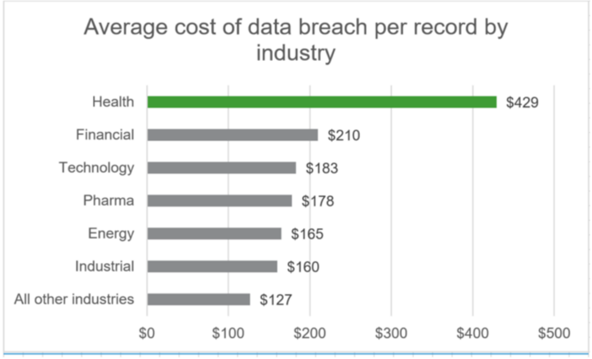
- Electronic health records (EHR) for patients, instead of paper records.
- Secure digital networks to send and deliver up-to-date records whenever and wherever the patient or clinician may need them.
- Electronic transmittal of medical test results.
- Confidential and secure patient health portals for patients to access their personal health information online.
- Mobile devices and tablets to update patient records in real time and document at the point of care.
- Telemonitoring applications that allow patients to transmit vitals or diagnostic information to providers remotely.

2. Impacts of Security gaps

Healthcare data breaches hit all time high in 2021, impacting 45M people. While we continue to rave about how Artificial Intelligence (AI)/(Electronic health records (EHRs) can improvise rural healthcare. Healthcare remains costliest industry for data breaches. While electronic health records (EHRs) offer incredible advantages for quickly accessing patient data, eliminating fragmentation, and improving information sharing, they also present security challenges. As statics show. a shocking 41,335,889 patient records were leaked during data breaches in recent times. this raises grave concerns about the Patient data security.

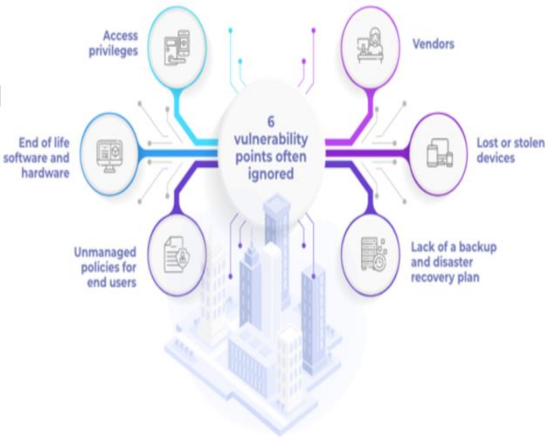
Patient data breaches occur due to both internal and external attacks, such as hacking, theft/loss, unauthentic internal disclosure, and the improper disposal of unnecessary but sensitive data. However, hacking/IT incidents are most used by attackers. Furthermore, the Email and Network servers are the main locations from where confidential health data is beached. healthcare data breaches are far more expensive than the average cost of data breaches.





3. Analyzing of Security gaps in rural healthcare

While rapid increase in digitization of rural healthcare is welcome transformation, many a times, the lack of policies and access control leads to staggering amount of Patient Data compromise and breaches at multiple levels that include identity theft and financial threat. Threat management is a major challenge to all healthcare organizations especially in rural communities Most common vulnerability often ignored are:


6 vulnerability points often ignored
Access privileges
Vendors
End of life software and hardware
Lost or stolen devices
Unmanaged policies for end users
Lack of a backup and disaster recovery plan

1. **Access privileges:** Unmanaged firewall configurations and remote access, lack of access policies for employees and vendors.
2. **End of life software and hardware:** Vendors stop providing patches and using out-of-date and high-risk technology such as java applets.
3. **Unmanaged policies for end users:** Lack of website control and application download control, sharing credentials, etc.
4. **Vendors:** Hospitals work with vendors (insurance companies, etc.) without assessing the accompanying security risks.
5. **Lack of a backup and disaster recovery plan:** The quickest way to recover from an attack is to rebuild all the breached systems. A good backup and recovery plan can help.

Healthcare security is always at the mercy of the multiple cyber threats listing a few recent incidents.

- 34% of the respondents were affected by ransomware attacks in the last year.
- 5% of those affected had their data encrypted by the cybercriminals.
- 34% of those whose files had been held hostage via encryption paid the ransom, with the total losses amounting to an average of US$1.27 million.
- Only 24% of the participants do not expect to be hit by a ransomware attack within the next year.

Recent healthcare security issues highlight the use of emerging technology is creating these.

Ransomware scams: Ransomware remains one of the biggest challenges healthcare faces.
Hacktivism: With many hacker groups and Anonymous roaming the digital land, patient data security is always at risk.
User error: Sending unencrypted medical data over email or in messages is a surefire way to lose it in a cyberattack. Even better: sending one's access credentials or storing them in a simple Google doc.
Use of legacy technology: As it turns out, using older technology can't guarantee the security of your patients' data either. Outdated software can be a major source of security issues in Healthcare.
Adoption of cloud technology and mobile apps: The issue with cloud and mobile tech mainly has to do with on-the-fly encryption of the data that's constantly traveling between servers and devices.

4. Role of Emerging Technology in Securing Patient Data

Digital Transformation in rural healthcare is all about adopting new age technologies to deliver efficient patient care backed by robust and secure systems that enable instant and secure access to patients 'data across platforms. Building a strong line of defense based on the emerging technologies to counter cyberattacks and security vulnerabilities is extremely important. As a result, it is crucial that organizations implement healthcare data security solutions that will protect important assets while also satisfying healthcare compliance mandates. Various technologies are in use for protecting the security and privacy of healthcare data. Most widely used technologies are:

Authentication: Authentication is the act of establishing or confirming claims made by or about the subject are true and authentic. It serves a vital function within any organization: securing access to corporate networks, protecting the identities of users, and ensuring that a user is who he claims to be. Most cryptographic protocols include some form of endpoint authentication specifically to prevent man-in-the-middle (MITM) attacks. For instance, Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet.
TLS and SSL encrypt the segments of network connections at the Transport Layer end-to-end. Several versions of the protocols are in widespread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voiceover-IP (VoIP). One can use SSL or TLS to authenticate the server using a mutually trusted certification authority. Additionally, Bull Eye algorithm can be used for monitoring all sensitive information in 360° . This algorithm has been used to make sure data security and manage relations between original data and replicated data. It also allows only authorized person to read or write critical data. Paper [13] proposes a novel and a simple authentication model using one time pad algorithm. It provides removing the communication of passwords between the servers. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at the entry of every access.

Encryption: Data encryption is an efficient means of preventing unauthorized access of sensitive data. Its solutions protect and maintain ownership of data throughout its lifecycle — from the data center to the endpoint (including mobile devices used by physicians, clinicians and administrators) and into the cloud. Encryption is useful to avoid exposure to breaches such as packet sniffing and theft of storage devices. Rural Healthcare organizations must ensure that encryption scheme is efficient, easy to use by both patients and healthcare professionals and easily extensible to include new electronic health records. Furthermore, the number of keys owned by each party should be minimized.

Although various encryption algorithms have been developed and deployed relatively well (RSA, Rijndael, AES and RC6 [14, 16, 17], DES, 3DES,RC4 [15], IDEA, Blowfish …), the proper selection of suitable encryption algorithms to enforce secure storage remains a difficult problem.

Data Masking: Masking replaces sensitive data elements with an unidentifiable value, but is not truly an encryption technique so the original value cannot be returned from the masked value. It uses a strategy of de-identifying the data sets or masking personal identifiers such as name, social security number and suppressing or generalizing quasi - identifiers like data-of-birth and zip-codes.

Thus, data masking is one of the most popular approaches to live data anonymization. k-anonymity first proposed by Swaney and Samrati [18, 19] protects against identity disclosure but failed to protect against attribute disclosure. Truta et al. [20] have presented p-sensitive anonymity that protects against both identity and attribute disclosure.

Other anonymization methods fall into the classes of adding noise to the data, swapping cells within columns and replacing groups of k records with k copies of a single representative. These methods have a common problem of difficulty in anonymizing high dimensional data sets [21, 22]. A significant benefit of this technique is that the cost of securing a big data deployment is reduced. As secure data is migrated from a secure source into the platform, masking reduces the need for applying additional security controls on that data while it resides in the platform.

Access Control: Once authenticated, the users can enter an information system, but their access will still be governed by an access control policy which is typically based on the privilege and right of each practitioner authorized by patient or a trusted third party. It is then, a powerful and flexible mechanism to grant permissions for users. It provides sophisticated authorization controls to ensure that users can perform only the activities for which they have permissions, such as data access, job submission, cluster administration, etc.

Several solutions have been proposed to address the security and access control concerns. Role-Based Access Control (RBAC) [23] and Attribute-Based Access Control (ABAC) [25, 26] are the most popular models for EHR. RBAC and ABAC have shown some limitations when they are used alone in medical system. Paper [24] proposes also a cloud oriented storage efficient dynamic access control scheme cipher text based on the CP-ABE and symmetric encryption algorithm (such as AES). To satisfy requirements of fine-grained access control yet security and privacy preserving, we suggest adopting technologies conjunction of other security techniques, e.g., encryption, and access control method.

Additionally, data protection laws are more than ever crucial in healthcare organizations to manage and safeguard personal information and address their risks and legal responsibilities in relation to processing personal data, to address the growing thicket of applicable data protection legislation. Different countries have different policies and laws for data privacy. Data protection regulations and laws in some of the countries along with salient features are listed in the Table below.

Data protection laws in some of the countries:

Country	Law	Salient Features
U.S.A	HIPAA Act Patient Safety and Quality Improvement Act (PSQIA) HITECH Act	Requires the establishment of national standards for electronic health care transactions. Gives the right to privacy to individuals from age 12 through 18. Signed disclosure from the affected before giving out any information on provided health care to anyone, including parents. Patient Safety Work Product must not be disclosed [27]. Individual violating the confidentiality provisions is subject to a civil penalty. Protect security and privacy of electronic health information.

EU	Data Protection Directive	Protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data. [29]
Canada	Personal Information Protection and Electronic Documents Act ('PIPEDA')	Individual is given the right to know the reasons for collection or use of personal information, so that organizations are required to protect this information in a reasonable and secure way.[28]
UK	Data Protection Act (DPA)	Provides a way for individuals to control information about themselves. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.
Russia	Russian Federal Law on Personal Data	Requires data operators to take "all the necessary organizational and technical measures required for protecting personal data against unlawful or accidental access".
India	IT Act and IT (Amendment) Act	Implement reasonable security practices for sensitive personal data or information. Provides for compensation to person affected by wrongful loss or wrongful gain. Provides for imprisonment and/or fine for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract.
Angola	Data Protection Law (Law no. 22/11of 17 June)	With respect to sensitive data processing, collection and processing is only allowed where there is a legal provision allowing such processing and prior authorization from the APD is obtained.

Conclusion

Limitless opportunities are offered to drive health research, knowledge discovery, clinical care, and personal health management. However, there are several obstacles and challenges that impede its true potential in the rural healthcare field, including technical challenges, privacy and security issues and skilled talent. Big data security and privacy are considering as the huge Privacy and security issues.

In addition of the methods currently used to ensure patient's privacy in rural healthcare, there are more various techniques include Hiding a needle in a haystack [30], Attribute based encryption Access control, Homomorphic encryption, Storage path encryption and so on. However, the problem is always imposed. In this context, as our future direction, perspectives will focus more on achieving effective solutions to the scalability problem of privacy and security in the area of rural healthcare. Also multiple designs and frameworks can be implemented to solve the problem of reconciling security and privacy models by simulating diverse approaches using exploiting the MapReduce framework. To, ultimately, support decision making and planning strategies, for a robust rural healthcare infrastructure.

References

1. https://www.hipaajournal.com/category/healthcare-data-security/
2. https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people
3. https://www.mdpi.com/2227-9032/8/2/133/htm
4. https://www.futurismtechnologies.com/solutions/futurism-data-protect-services/
5. https://www.cdwg.com/content/cdwg/en/industries/healthcare-technology/rural-healthcare.html
6. “State Of Enterprise IoT Security: A Spotlight On Healthcare”, Forrester Consulting, September 2019.
7. “Largest Healthcare Data Breaches of 2021”, HIPPA Journal, December 2021.
8. “Ransomware attack on Georgia health system endangers info of 1.4M patients”, Healthcare IT News, August 2021.
9. “Takeover of a Spacelabs Xprezzon Patient Monitor Demo”, Armis.
10. “URGENT/11: II Zero Day Vulnerabilities Impacting VxWorks, the Most Widely Used Real-Time Operating System (RTOS)”, Armis, August 2019
11. “TLStorm: Three critical vulnerabilities discovered in APC Smart-UPS devices can allow attackers to remotely manipulate the power of millions of enterprise devices”, Armis, 2022.
12. https://demigos.com/blog-post/data-security-in-healthcare-importance-challenges-solutions/
13. C. Yang, W. Lin, and M. Liu, "A Novel Triple Encryption Scheme for Hadoop-Based Cloud Data Security," in Emerging Intelligent Data andWeb Technologies (EIDWT), 2013 Fourth International Conference on, 2013, pp. 437-442.
14. Federal Information Processing Standards Publication 197,"Specification for the Advanced Encryption Standards (AES)", 2001.
15. S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key schedualing algorithm of RC4", 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK, 2001.
16. J. Shafer, S. Rixner, and A. L. Cox. The Hadoop Distributed File system: Balancing Portability and Performance. Proc. of 2010 IEEE Int. Symposium on Performance Analysis of Systems & Software (ISPASS), March 2010, White Plain, NY, pp. 122-133.
17. N. Somu, A. Gangaa, and V. S. Sriram, "Authentication Service in Hadoop Using one Time Pad," Indian Journal of Science and Technology, vol. 7, pp. 56-62, 2014.
18. L. Sweeney, “Achieving k-anonymity privacy protection using gener- alization and suppression,” in International journal on uncertainity, fuzziness and knowledge based systems, vol. 10, 2002, pp. 571 – 588.
19. P. Samrati, “Protecting respondents identities in microdata release,” in IEEE transactions on knowledge and data engineering, vol. 13, 2001, pp. 1010 – 1027.
20. T. M. Truta and B. Vinay, “Privacy protection: p-sensitive k-anonymity property,” in Proceedings of 22nd International Conference on Data Engineering Workshops, 2006, p. 94.
21. N. Spruill, “The confidentiality and analytic usefulness of masked business microdata,” in Proceedings on survey research methods, 1983, pp. 602–607.
22. S. Chawala, C. Dwork, F. M. Sheny, A. Smith, and H. Wee, “Towards privacy in public databases,” in Proceedings on second theory of cryptography conference, 2005.
23. Science Applications International Corporation (SAIC). Role-Based Access Control (RBAC) Role Engineering Process Version 3.0. 11 May 2004.
24. H. Zhou and Q. Wen, "Data Security Accessing for HDFS Based on Attribute-Group in Cloud Computing," in International Conference on Logistics Engineering, Management and Computer Science (LEMCS 2014), 2014.
25. A. Mohan, D. M. Blough, An Attribute-Based Authorization Policy Framework with Dynamic Conflict Resolution, Proceedings of the 9th Symposium on Identity and Trust on the Internet, 2010.
26. M. Hagner. Security infrastructure and national patent summary. In Tromso Telemedicine and eHealth Conference, 2007. 2

27. Data Protection Laws of the World. 2017 DLA Piper. [Online]. Available: http://www.dlapiperdataprotection.com 2
28. Challenges of privacy protection in Big Data Analytics –Meiko Jensen- 2013 IEEE International Congress on Big Data. 2013.
29. Privacy and Big Data – Terence Craig & Mary E.Ludloff
30. Jung K, Park S, Park S. Hiding a needle in a haystack: privacy preserving Apriori algorithm in MapReduce framework PSBD'14, Shanghai; 2014. p. 11–17.