Secure health care messaging in the era of COVID-19

Aug 27, 2020 Save This ()

Duncan Rozario Duncan Rozario

Business and health care data are the new “honeypot,” an attractive and lucrative source of revenue to the modern hacker. A report from IBM (https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year) in July 2020 reported that the average cost of a health care breach was $7.13 million per breach, noting “compromised employee accounts were the most expensive root cause, and that 80% of these incidents resulted in the exposure of customers' personally identifiable information.”

The COVID-19 pandemic has exposed how unprepared many health care providers were to provide virtual care and create a virtual front desk. Integrated systems, such as Kaiser Permanente in the U.S., developed the infrastructure years ago and already conducts more than half of its 100 million patient encounters virtually, 80% of which (https://www.healthcaredive.com/news/virtual-care-moves-toward-the-frontline-of-provider-patient-relationships/516025/) is done with secure messaging. How prepared is health care to engage with patients using modern secure email?

In their 2018 report (https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/E-Brief%20277.pdf) for the C.D. Howe Institute, Sacha Bhatia and William Falk proposed a “virtual first” philosophy that uses virtual visits and secure email to provide care whenever possible. They emphasize the importance of adopting secure email to communicate between care providers and patients. A study from the Journal of Academic Medicine (https://www.mcgaw.northwestern.edu/docs/Email-Communication-Among-Providers-Guidelines.pdf) identified that more than 90% of those surveyed felt patient care was improved as a result of email use due to the efficiency of email communication. Despite its use in health care, modern conventional email is not a secure method to transmit personal health information.

The Information and Privacy Commissioner of Ontario stated in 2016 (https://www.ipc.on.ca/resource/fact-sheet-communicating-personal-health-information-by-email/) that the Personal Health Information Protection Act requires the use of encryption, stating, “The IPC expects that email communication of personal health information among custodians will be secured from unauthorized access by use of encryption” and “custodians should use encryption for email communication with patients.”

Modern email

Modern email is a federated system of communication that uses the Simple Mail Transfer Protocol to send written communication from the author, though independent services, to the recipient. SMTP is an internet standard that manages the flow of more than 188 million emails (https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/) per minute in 2019 around the world. At the client level, IMAP and POP3 are standards for retrieving emails from the server. While SMTP handles the ASCII-level email, the Multipurpose Internet Mail Extensions was developed to transfer binary files, such as images.

The author’s communication to the Message Submission Agent is protected by Transport Layer Security (the current version is TLS 1.3 defined in RFC 8446) (https://www.rfc-editor.org/info/rfc8446), but that is valid for only one Transmission Control Protocol hop (https://kb.iu.edu/d/beha#:~:text=When%20you%20send%20an%20email,between%20you%20and%20your%2(The email with its header (metadata) and body is transmitted in plaintext for the subsequent TCP hops, allowing for easy interception. A compromise of the server would allow unauthorized access to the message, metadata or TLS keys, rendering future TLS communication insecure.

Hazards of email

Despite the wide-spread utilization of email, its privacy concerns are often underestimated as email messages are not encrypted; they are transmitted in plaintext through multiple intermediaries that can read or alter the message, copies of the messages are often stored on multiple devices en route, web beacons embedded in the email can alter the sender when the email is read and from which IP address, emails routed through internal mail systems can be read by IT personnel, header fields such as sender origin can be spoofed to facilitate spam and they expose sensitive information, no integrity checks to ensure that the message is not modified en route, and viruses and other malicious code can be embedded in the email.

Modern encryption

As a privacy professional, what should you be looking for in a secure messaging platform to ensure that protected health information and confidential business information remain secure?

End-to-end encryption

End-to-end encryption (https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work) allows communication to be completely secured along the full data path. While TLS keys secure the transmission from client to server, public-key encryption, such as the Rivest–Shamir–

Adleman, allows the data to be secured on the server at all times. Private keys need to be secured. Advanced Encryption Standard (https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences) is the same and used for encryption and decryption. An asymmetric key, such as RSA, is used to secure this symmetric key and ensures that the message is not altered en route. Does the provider automatically update encryption algorithms without user action? Is the encryption done at the client level (better) or server-side (worse)?

No passwords in plaintext

Passwords and private keys need to be encrypted at all times. This way, the password and private key itself cannot be reverse engineered with access to the server. Instead of hash functions, pseudorandom function families use keys to map secure information to data that is indistinguishable from random.

Metadata security

The header contains data, such as origin email, date, destination email, cc, subject, Authentication-Results, DKIM-Signature, routing information and delivery parameters, which supply a great deal of information about the email. Is this fully secured in the solution you are assessing?

Forward security flaw

While your current RSA key pairs may provide adequate security, intelligence organizations may store large volumes of encrypted emails in the hope that the private key may be obtained in the future or that the encryption algorithm is broken. Does your provider have a solution for this?

2FA

Two-factor authentication is another layer of security that combines something you know (password) with something you have (e.g., cellphone to receive an SMS or token generator) to increase the security of authentication.

Compliance audit

Has an accredited external organization audited the organization's compliance with security and regulatory guidelines? Does the provider meet the requirements of PHIPA, Canada's Personal Information Protection and Electronic Documents Act or the U.S. Health Insurance Portability and Accountability Act?

Data sovereignty and physical security

The physical location of your server's data center and data path of your information now have a significant impact on security. What is the physical location of the server, and how does the data get to you? What are the data protections of that country? Certification, such as ISO 27001 and SOC2 (https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html), provides an external audit of physical security, availability, processing integrity, confidentiality and privacy.

Quantum encryption

Modern encryption is based on the fact that complex algorithms take a long time to crack with current computing power, but the advent of quantum computers puts these at risk. The RSA-2048 bit encryption (https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/#:~:text=It%20would%20take%20a%20classical,RSA%2D2048%20bit%20encryption%20key) that would take current systems millions of years to break could be broken in hours with a quantum computer with 20 million qubits, a system that does not yet exist.

Conclusion

In the Notification of Enforcement Discretion (https://iapp.org/media/pdf/resource_center/telehealth_hipaa_covid19_faq.pdf) issued by the U.S. Department of Health and Human Services' Office for Civil Rights, "Covered health care providers will not be subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules that occur in the good faith provision of telehealth during the COVID-19 nationwide public health emergency." As we move into the post-COVID-19 era, how will we move from insecure to secure messaging to ensure the privacy and security of our health care system? As we are still in the middle of our pandemic, we need to rapidly pivot to available technology to ensure that we can physically distance yet provide compassionate care with privacy and security.

Whether virtual care is here to stay will depend upon not only remuneration, but also on customer confidence in security and privacy (https://www.nytimes.com/2020/08/03/health/covid-telemedicine-congress.html). Ann Cavoukian, executive director of the Global Privacy and Security by Design Centre and former three-term information and privacy commissioner of Ontario, has said, "those organizations that prioritize the privacy of their customers gain a corresponding competitive advantage; by actively protecting the integrity of customer data and supporting consumer privacy, companies not only realize meaningful economic benefits, but also build greater trust and create deeper customer connections."

Rather than mere compliance with existing regulations, an aspiration to excellence has the potential to move the goalposts to optimize the consumer experience and vault businesses to the top of the race for privacy and security leading to business success.

Photo by Tom Claes on Unsplash

Approved CIPM, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPT Credits: 1