Sponsored by:

How fighting cyberattacks and improving the patient experience can help secure all healthcare stakeholders during COVID and beyond

As the healthcare industry rises to the challenge of COVID-19, health systems data and patient records are under growing attack. Our industry has long been an attractive target for hackers—who can get $250 on the dark web for each stolen patient record, compared to $5.40 for a payment card and only 53 cents for a social security number. Now the pandemic has led to a precipitous rise in cyberattacks, ransomware, and malware, as everyone now relies on online services and digital interactions, including many less computer-savvy consumers. Coinciding with a greater number of new users, fraudsters are becoming more sophisticated. But blunt security measures that attempt to "lock down" medical records are rarely effective against clever cybercriminals, but they do frustrate patients who struggle to remember usernames and passwords.

To help the healthcare industry defend against aggressive cyber criminals, while providing patients the best user experience, we talked with two Mastercard experts in information security and data management, who suggested the following best practices:

Assess and mitigate cyber risk

Organizations need to follow good cyber hygiene as they adopt the digital transformation wave and adapt to new norms. Ashish Gupta, a Vice President with Mastercard Advisors focused on Cybersecurity, knows the healthcare industry well, having served as CISO for a digital health data exchange in his career. Gupta explained the escalation of cyber threats is largely due to increased exposure: "The pandemic has resulted in more healthcare staff working remotely or using personal devices that may not be managed or secured by the hospital IT team," says Gupta. "Where before they had secure access to sensitive data within the relatively secure walls of their offices, now employees, contractors, and other partners must access that data through new channels, which are often not as secure." It's no wonder that most organizations' IT groups are overwhelmed.

"The new normal ushered in by COVID-19 has greatly expanded the attack surface—the points of vulnerability for healthcare organizations—and likewise expanded cyber risk," explains Gupta. He recommends CISOs review their data use and protection processes and controls to:

- **Protect** your data assets – reevaluate how you classify and access data; it must be readily available to maintain business as normal, but with greater controls to ensure responsible and governed use. Reduce the data you collect to the minimum necessary, and ensure that proper checks are in place through the data's lifecycle to protect it physically (storage, backups, portability), and virtually (access, usage, encryption). This will help reduce your attack surface.
- **Prioritize** cybersecurity initiatives – diagnose real-world threats your organization faces and assess your defenses against them, to invest in security initiatives with the highest ROI and to optimize the use of your limited resources.
- **Practice** for the breach – prepare your team to respond to a cyber incident/breach both from technical and managerial perspectives to help reduce your response and recovery times.
- **Prevent** the attack – coach your workforce to be cybersecurity-aware with frequent and relevant reminders to reduce the likelihood of a successful cyberattack or cyber incident.

"These concepts are not new and most healthcare organizations have adopted elements of them," says Gupta. "However, those who quickly implement these 4-Ps will be able to overcome cyberattacks, while laggards will likely be overcome by them." Mastercard Advisors Cybersecurity services can help you determine which steps will give your organization the highest ROI.

Improve patient experience—and security

The high incidence of fraud in healthcare has prompted providers to introduce severe security measures to verify patients. But very narrow rules introduce their own problems, as Micheal Pettibone, Vice President of Cyber & Intelligence Solutions with over 20 years' experience in identity, explains: "Most of these security measures cause patients a high degree of friction, frustrating their attempts to access medical records or lab results. Requiring a patient to remember their username/password for a health system they rarely use is just a bad customer experience." Compounding the problem, says Pettibone, "is that more systems are being interconnected, due to the CMS Interoperability and Patient Access rule, plus patients want greater access to their digital medical records—which creates even more vulnerable access points."

"Naturally, we must protect patients' medical records," admits Pettibone, "but the present method is burdensome to patients." And with telemedicine skyrocketing as the pandemic shut down doctors' offices and clinics across the country, health providers struggle to validate that patients are who they claim to be. Pettibone recommends CISOs review the UX to consider:

- **Biometrics** for patient portal login – providing both a seamless login experience and easy access to medical records, while increasing an organization's overall security posture.
- **Mobile-first** strategy – patients want to manage their health on their mobile device—be it telemedicine with a doctor or accessing medical records. And mobile devices bring an added benefit: the ability to use behavioral biometric data (device "finger printing") for higher assurance the patient is who they claim.
- **Artificial intelligence** – providers have saved millions of dollars per year and countless patient hours by detecting fraudulent claims using AI. Beyond the cost of fraud, the last thing a provider wants is to lose a patient after their identity is stolen.

Verifying a patient's identity used to be difficult and cumbersome, but "with Mastercard technology," Pettibone says, "you can offer patients a better overall experience while also providing a higher level of assurance."

Contact healthcaresolutions@mastercard.com to learn how Mastercard is bringing its expertise to healthcare, or visit mastercard.us/healthcare-solutions