CME

MARSHALL FRIEDEN, MD, ISABEL STRAW, MD, BMBS, MPH, PhD, NICOLAS KAHL, MD, NATHAN YUNG, MD, GRANT MADDEN, CHRISTIAN DAMEFF, MD, MS, AND JEFFREY TULLY, MD

Cybersecurity Preparedness and Resiliency in a Family Medicine Clinic

With ransomware attacks increasingly targeting health care institutions, practices must protect themselves by developing a cybersecurity response plan.

Cyberattacks targeting health care organizations have increased in scope and impact over the last decade. These include "ransomware" attacks in which hackers lock organizations out of their own internet-connected files, systems, or networks until they pay a ransom. These attacks disrupt patient care and stress regional health care ecosystems.[1,2]

The February 2024 cyberattack on Change Healthcare, a UnitedHealth Group subsidiary, demonstrated how such attacks can not only impact one hospital or health system but also ripple across all health care sectors due to consolidation in the industry. While much of the literature focuses on cyberattacks disrupting care for acute emergencies such as heart attack, stroke, or sepsis,

ABOUT THE AUTHORS
Dr. Frieden is a family physician and clinical informatics fellow at UC San Diego Health. Dr. Straw is an emergency physician and assistant professor of healthcare artificial intelligence and cybersecurity at University College London. Dr. Kahl is an emergency physician and clinical informatics fellow at UC San Diego Health. Dr. Yung is an internal medicine physician at UC San Diego Health. Grant Madden is emergency manager at the UC San Diego Center for Healthcare Cybersecurity. Dr. Dameff is an emergency medicine physician and assistant professor in the Department of Medicine Division of Biomedical Informatics at UC San Diego Health. Dr. Tully is an associate clinical professor of anesthesiology at the UC San Diego School of Medicine and co-director of the UC San Diego Center for Healthcare Cybersecurity. Author disclosures: no relevant financial relationships.

they can also cause serious problems for patient health and clinic finances in primary care.[3,4] Family medicine clinics increasingly rely on systems connected to the internet — EHRs, pharmacy portals, laboratory systems, clinical image viewers, etc. — and the abrupt absence of these tools can drastically disrupt workflows if the practice is not prepared. Scheduled downtime intended for brief updates to computer systems is not sufficient preparation for cyberattacks, which can affect multiple technological systems for weeks or even months with no warning.[5,6]

Preventing cyberattacks requires a detailed, multipronged approach that is beyond the scope of this article (for that, we recommend this 2023 federal report: https://405d.hhs.gov/Documents/HICP-Main-508.pdf). Below, we offer guidance on how practices can keep patient care and revenue flowing even if a cyberattack causes prolonged tech outages.

CREATING A CYBERSECURITY RESPONSE PLAN

Clinics should prepare for the possibility of cyberattacks by creating a cybersecurity response plan, which involves the following:

1. Identify workflows with tech vulnerabilities. List the key workflows your practice follows before, during, and after a patient visit, and identify those that rely on internet-connected systems. This includes scheduling patients, accessing their contact information, checking patients in and out, processing orders (for referrals, labs, imaging, medications/refills, etc.), documenting visits, billing payers and patients, and reporting quality metrics.

2. Make technology-independent backup plans. When you have identified that a cyberattack has occurred, you will want to disconnect any affected devices in collaboration with your clinic's IT service provider and move to alternative workflows. As part of your current downtime procedures for regular IT maintenance, you likely have a number of backup processes in place. Consider whether they are adequate to withstand a prolonged disruption due to cyberattack and what additional backup plans you need to create.

For example, paper forms for ordering labs, billing payers, or documenting visits that you may have stocked to cover just a brief scheduled outage may need to be expanded to bridge weeks or even a month. The information you document on these paper forms can be logged in the EHR after the cyberattack is resolved and online systems are restored.

Another example is your clinic schedule. Many clinics now use internet cloud-hosted scheduling software, which may not be accessible during a cyberattack. Having a backup schedule — a regularly updated offline schedule with patients' appointment times and contact information as well as staffing schedules for a fixed future increment (e.g., a month) — will alleviate confusion and difficulty during a cyberattack. Designate a staff member to print a copy or save it to their computer's hard drive (not to the network or cloud) at the end of each work day.

> Scheduled downtime intended for brief updates to computer systems is not sufficient preparation for cyberattacks.

3. Identify alternative communication systems. Your clinic's communication systems also may be disrupted during a ransomware attack. Cyberattacks can lock you out of your email system and may cause outages of Voice over Internet Protocol (VoIP) phone and e-fax services as well. If your practice uses those, have a backup plan that protects patient privacy, whether that's maintaining a single non-VoIP

KEY POINTS

- Cyberattacks on health care organizations are increasing, and family medicine clinics should prepare for the possibility of prolonged technological outages.
- Practices should create a cybersecurity plan that identifies workflows with tech vulnerabilities and outlines technology-independent backup plans.
- Practices should test their cybersecurity plan each year with a simulated cyberattack and update the plan as they introduce new technology.

KEY MEMBERS OF A CYBERSECURITY TEAM

- Coordinator (such as an office manager): oversees the plan, coordinates contributors, and ensures compliance;
- Physician: makes clinical decisions and liaises with other external medical services;
- Administrative staff member: creates, manages, and stores patient documentation in the absence of applications and systems;
- Facilities expert (such as an engineer from the building management team): oversees utilities (electricity, water, sewer, telephone, gas, and heat) for the practice that may be affected during a cyberattack;
- IT rep (someone from your parent organization, internet service provider, or contracted IT consultant): serves as the point of contact for all internet connections.

phone/fax number or having staff use personal devices with encrypted apps such as Signal (for audio calls), Doctolib Siilo (for text messaging), and Proton Mail (for email). Although HIPAA does not require encrypted communication, it is recommended practice.[7]

Cyberattacks can also cause a clinic's telemedicine system to go down. If telemedicine is a key part of your practice, designate someone with clinical expertise who can triage those appointments in the event of a cyberattack, deciding which can be rescheduled and which should be converted immediately into in-person visits.[8]

4. Have a plan for seeing patients. Even with proper preparation, the transition to offline processes may temporarily reduce your clinic's capacity to see patients. Establish procedures for triaging, cancelling, or rescheduling in-person appointments as needed, and identify offline ways to communicate with individual patients about their appointments (e.g., non-VoIP phone) and with the public at large about your facility's capacity to accept walk-ins (e.g., putting a sign on the door or notifying local media). Identify a facility or facilities to serve as a referral site if the disruption to your operations is substantial enough to prevent basic care or services, such as requests for prescription refills. With a proper plan in place, practices should expect this level of disruption to last no more than a day or two.

5. Identify at-risk patient groups. Certain patient populations may be at risk of disproportionate harm from a cyberattack. Consider maintaining an offline database of these patients and their contact information so you can prioritize their care, and designate a staff member to notify them of how to get in touch with you if you have had to move to alternative communication systems. Vulnerable patients may include the following:

• Patients with unstable chronic conditions for whom cyberattacks may disrupt essential physiological monitoring[9] (hospital staff might be able to order in-house imaging or labs through a runner or paper forms during a cyberattack outage, but outpatient clinics without such services will need to make plans to order testing without internet-connected systems),

• Patients scheduled for follow up after a hospital admission or emergency room visit (whose care likely relies on the ability to access lab studies, medication prescriptions, and hospital records, which may be less accessible during a ransomware attack),

• Newborn patients (cyberattacks may hinder a clinic's ability to register new births, complicating follow up for these patients[5]), particularly those with conditions such as hyperbilirubinemia discharged from the hospital on the assumption that an outpatient clinic can monitor their bilirubin level (in the event of a cyberattack, the discharge weight and previous bilirubin levels may be unknown, which can make a critical difference in the decision to send a baby to the ER, initiate home phototherapy, or continue to monitor as an outpatient),

• Patients late in pregnancy for whom cyberattacks can impact birth procedures (e.g., loss of access to blood products and surgical theatres leading to cancellation of planned C-sections and changes to labor plans for pregnant mothers[10]),

• Patients in cancer treatment (cyberattacks may prevent radiation-guided treatment, block access to cloud-based chemotherapy platforms, and force clinicians to try and reconstruct complex cancer treatment regimes from memory[11]),

• Palliative care patients (a shutdown of IT systems during a cyberattack can cause difficulties in accessing important palliative information and medications, leading to obstructed care at a critical time for these patients and their families).

6. Prepare to continue business operations without online systems. All cybersecurity preparedness plans should include a process that allows the practice to temporarily convert to paper billing. Insurance companies may have strict timelines for filing claims and supporting documentation and could deny late filings even if the delay was due to a cyberattack. Practices can prepare by storing preprinted billing documents with a list of each insurer's fax number and mailing address in a secure box onsite.

Practices should also prepare for the possibility that they will be unable to accept payments from patients electronically or in-person via credit card during a cybersecurity event. Practices may choose to defer these payments until electronic services are restored, but they still need an offline way to track what's owed. This requires having paper documents that include a place to write account balances and a space for the patient's signature acknowledging the debt (carbon copy forms allow you to give one to the patient as well as keep one for the practice's records). If deferring patient payments will cause too many cashflow difficulties, work with a credit card servicer that offers offline processing.[12]

IMPLEMENTING THE CYBERSECURITY RESPONSE PLAN

Once you have developed a cybersecurity response plan, you need to test it, as you would with a fire drill. Running cybersecurity "tabletop exercises," or simulations, helps practices find weaknesses in their response plan and helps the cybersecurity response team (see page 28) get comfortable filling their roles. Larger practices may have an in-house IT team that can design such a simulation. Smaller practices can use national guidance and existing research studies as templates.[13,14]

As with all emergency preparedness plans, cybersecurity drills should be performed and reviewed yearly and updated when a clinic adopts new technology (e.g., VoIP phones). If a practice is part of a health care system, cybersecurity plans will need to align with the response plan of the larger institution. Points of contact to coordinate plans include an organization's chief information security officer (CISO) or emergency manager.

While a response plan can help clinics safely continue operations during a cyberattack, it does not address the cyberattack itself. For that, practices should contact their IT teams, as well as their local FBI office and the federal Cybersecurity and Infrastructure Security Agency (CISA). CISA is the one-stop location for reporting cybersecurity events through their portal page at https://myservices.cisa.gov/irf, via email at SayCISA@cisa.dhs.gov, or by phone at 1-844-Say-CISA. Since 2022 the Cyber Incident Report for Critical Infrastructure Act (CIRCIA) has required "covered entities" to report cybersecurity and ransomware events to CISA within 72 hours. Your response plan should assign one member of the cybersecurity team to do this.

> All cybersecurity plans should include a process that allows the practice to temporarily convert to paper billing.

Having a plan and drilling it regularly should give practice staff more confidence in their ability to weather a cyberattack, but it's still likely to be stressful if one occurs. Just as you check in on your at-risk patients, it may be worthwhile to check in on your staff to inquire about burnout. It may also be helpful to let them know that you have contacted authorities and keep them updated on any developments in the attack investigation, as well as any potential timeline for restoring affected systems and returning to normal processes.

FUTURE DIRECTIONS

Cyberattacks in health care are still a relatively new phenomenon and further study is needed to establish standardized metrics to track post-attack clinical and financial outcomes and assess the efficacy of cyberattack preparedness plans. Our hope is that these recommendations will help raise the

Send comments to **fpmedit@aafp.org,** or add your comments to the article online.

cybersecurity awareness and resilience of family medicine clinics that constitute a key public health resource. While preparation will not prevent attacks, we believe it can reduce harm and keep practices operational. FPM

1. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on U.S. hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*. 2022;3(12):e224873.

2. Dameff C, Tully J, Chan TC, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the U.S. *JAMA Netw Open*. 2023;6(5):e2312270.

3. Pham TT, Loo TM, Malhotra A, et al. Ransomware cyberattack associated with cardiac arrest incidence and outcomes at untargeted, adjacent hospitals. *Crit Care Explor*. 2024;6(4):e1079.

4. Turner N. Family physicians: first point of contact, last line of defence. *Can Fam Physician*. 2023;69(7):490-491.

5. Abbou B, Kessel B, Ben Natan M, et al. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. *Front Digit Health*. 2024;6:1321485.

6. Neprash HT, McGlave CC, Rydberg K, Henning-Smith C. What happens to rural hospitals during a ransomware attack? Evidence from Medicare data. *J Rural Health*. 2024;40(4):728-737.

7. Alder S. HIPAA encryption requirements. *The HIPAA Journal*. Jan. 9, 2025. Accessed Feb. 25, 2025. https://www.hipaajournal.com/hipaa-encryption-requirements/

8. Romanovs A, Sultanovs E, Buss E, Merkuryev Y, Majore G. Challenges and solutions for resilient telemedicine services. Proceedings of the 2020 IEEE 8th Workshop on Advances in Information, Electronic and Electrical Engineering. Vilnius, Lithuania. https://www.researchgate.net/publication/351795369_Challenges_and_Solutions_for_Resilient_Telemedicine_Services

9. Duffy C, Murray C, Boran G, Srinivasan R, Kane A, Leonard A. Survey of Laboratory Medicine's national response to the HSE cyberattack in the Republic of Ireland. *Ir J Med Sci*. 2024;193(2):889-896.

10. NHS England. Weekly data on the impact of the Synnovis cyber-attack. Accessed Jan. 15, 2025. https://www.england.nhs.uk/london/synnovis-ransomware-cyber-attack/weekly-data/

11. Nelson CJ, Soisson ET, Li PC, et al. Impact of and response to cyberattacks in radiation oncology. *Adv Radiat Oncol*. 2022;7(5):100897.

12. Vasco N. Offline credit card processing: how to accept payments offline. Gravity Payments. July 5, 2023. Accessed Feb. 21, 2025. https://gravitypayments.com/blog/offline-credit-card-processing/

13. Straw I, Brass I, Mkwashi A, Charles I, Soares A, Steer C. Insights from a clinically orientated workshop on health care cybersecurity and medical technology: observational study and thematic analysis. *J Med Internet Res*. 2024;26:e50505.

14. Maggio LA, Dameff C, Kanter SL, Woods B, Tully J. Cybersecurity challenges and the academic health center: an interactive tabletop simulation for executives. *Acad Med*. 2021;96(6):850-853.

annfammed.org
ANNALS OF FAMILY MEDICINE
Home
Content
Info for
About
Engage
Contact
Careers
Review for AnnFamMed and earn Division II CME credit
ONLINE FIRST - Research & Video
LATEST ARTICLES
Voice Assistants and Cancer Screening: A Comparison of Alexa, Siri, Google Assistant, and Cortana
Voice assistants' answers to cancer screening questions vary
Current issue
NAPCRG
49th Annual Meeting
Nov. 19-23
REGISTER NOW