Baxter

# FIVE WAYS TO IMPROVE **CYBERSECURITY** IN THE PHARMACY

## Summary

Healthcare devices have become increasingly connected in the modern day pharmacy bringing gains in efficiency, safety, and clinical outcomes. However, digital innovations with increased connectivity have the potential to bring new vulnerabilities and increased exposure to cyber threats.

Cybersecurity in healthcare is unique due to the sensitivity of the data at risk and the potential life-threatening impacts of a cyberattack:

- Patient data rendered inaccessible.
- Life-saving medical equipment disabled.
- Delay and disruption to operations.

Healthcare cyberattacks are on the rise - the number of hacking incidents reported in healthcare increased by **42%** in 2020, climbing for the fifth straight year.[1]

The COVID-19 pandemic placed increased strain on already stretched healthcare systems and intensified global challenges of workforce capabilities, increasing patient acuity and the need to meet efficiency goals.

It is essential for pharmacies to implement cybersecurity measures to safeguard their connected systems and devices from cybercriminals. Pharmacists will benefit from knowing cybersecurity best practices within their area of control and understanding how to interact with IT for specialist support.

This paper discusses cybersecurity vulnerabilities and empowers pharmacists to take actions to address potential weaknesses, particularly when procuring new connected devices.

## Healthcare and cybersecurity

Healthcare today is increasingly reliant upon digital solutions – using data and connectivity of systems to optimize patient outcomes and create operational efficiencies. Personally identifiable information and protected health information (PHI) are handled by almost every hospital department.

Most healthcare providers use electronic health records, e-Prescribing software, remote patient monitoring, and/or laboratory information systems. For the pharmacy, connected systems play a vital role in the efficient and accurate delivery of drugs, which requires the modern pharmacist to have an awareness of what they can do to ensure the integrity of electronic data and ultimately protect the patients in their care.

While digital technologies undoubtedly contribute to healthcare improvements, they are at risk of being exploited through cyberattacks. Cybersecurity describes the various techniques used to protect private information by securing devices, electronic systems, networks, and data from malicious attacks. Cybersecurity in healthcare is unique due to the type of information stored and the potential consequences that can impact patient safety.

Given its wide range of misuse, from identity theft to medical fraud, an individual's PHI is more valued by cybercriminals than social security or credit card numbers and can sell for up to **20 times more** than this type of data.[2]

## The rise in cyberattacks

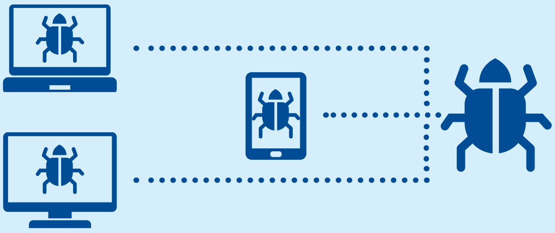
The noticeable increase in cyberattacks reflects the heavy targeting that healthcare received during the COVID-19 pandemic and it is believed that a considerable volume of data breaches have yet to be detected.[1,3] In the US alone, nearly 82% of healthcare records have been impacted by breaches since 2009.[4]

Healthcare data breach costs are on the rise, with the average cost of a single breach estimated to be **$9.23 million**, the highest of any industry.[5]

## The importance of and costs associated with cybersecurity

Cyberattacks can have significant financial implications, cause delay and disruption to sensitive hospital operations, and place patients' lives at risk. This is often done by strategically targeting connected devices.

The 2017 WannaCry software virus dramatically illustrated the public health threat posed by cybersecurity vulnerabilities. An example of a subset of malicious malware known as ransomware, WannaCry infiltrated computers by taking advantage of a software vulnerability in older versions of the Windows operating system, which Microsoft's regular security patches did not initially protect.[6] The virus then encrypted the information stored on the computer, rendering data inaccessible to its owner unless a ransom was paid.[7] The ransomware ultimately invaded hundreds of thousands of computers in more than 150 countries, including the UK's National Health Service (NHS) where normal operations of more than 80 individual hospitals were impacted for several days. Tens of thousands of scheduled surgeries and clinical appointments had to be canceled; complex medical equipment such as MRI machines and blood-product refrigerators were temporarily disabled; and in several areas, ambulances had to be diverted, resulting in delays in patient care.[7,8]



The NHS estimated the costs associated with the WannaCry attack to be at least **£92 million (US$115 million).**[9]

Medical devices can act as weak links in the cybersecurity chain and potentially allow malware to spread. Cybersecurity of these devices is critical yet their diversity can make it difficult to enact strict security policy. For the pharmacy, cyberattacks can increase risks to operations and patient safety and there is a clear need for clinical utility and safety to be balanced with security and privacy.

## Hospitals are responding to digital technology proliferation and the associated cybersecurity threats

Unlike other sectors, such as finance, healthcare has been comparatively late in establishing policies and dedicating resources to protect both data and its infrastructure. Connected medical devices, both in-hospital and off-site, have inherent limitations that expose them to cybersecurity vulnerabilities. They often lack the built-in resources to efficently employ security measures such as encryption, threat modeling, and malware detection.[10,11] Furthermore, unprepared for COVID-19 surges and heightened resourcing demands, many hospitals were forced to deprioritize important data protection measures, exacerbating the vulnerabilities that hackers have worked tirelessly for years to exploit.

For a healthcare facility to have a strong information security ecosystem, it requires quality IT or at least a stable application base and IT infrastructure.[12]

Cybersecurity should not be an afterthought, but one of the design requirements for medical device manufacturers.[13]

## Medical device manufacturers are increasing their focus on cybersecurity

> “The FDA is encouraging medical device manufacturers to take a proactive approach to cybersecurity management of their medical devices[14]”
>
> **Suzanne Schwartz,**
> Director of the Office of Strategic Partnerships and Technology Innovation at the U.S. Food and Drug Administaiton's (FDA) Center for Devices and Radiological Health (CDRH)

The FDA expects manufacturers to implement on-going lifecycle processes and to monitor continued safety post-market. In 2017, the FDA began mandating that medical device manufacturers show that their devices are able to have updates and security patches applied throughout their lifespan. Additionally, they must demonstrate that they have addressed any risks that would affect patients if the device were to be compromised.[15]

While these measures put the onus on manufacturers, hospitals should also be proactive in ensuring they are well protected against cybersecurity threats by investing in prevention, designating appropriate resources, and budgeting early, rather than depending on reactive approaches following attacks.

## Pharmacists have a role to play to protect themselves, the hospital, and patients

### 1. Elevate the pharmacy team's knowledge

Healthcare facilities' approach to cybersecurity should include the need to

**raise awareness and understanding**

among all users.[16,17]

End users, from clinicians to billing and scheduling staff, as well as patients and caregivers who connect their personal devices with the hospital network, can unintentionally or intentionally threaten the cybersecurity of the health facility.

To increase cybersecurity protection, pharmacies should frequently assess and identify knowledge gaps.[18] It is important for end users to realize the risks they may cause through inadvertent actions. For example, they should be aware that storing data on their mobile devices can pose privacy and data-integrity risks and using connected devices or removable storage devices can increase exposure to malware.[12,19] They should also be mindful of the importance of password privacy and protection.

End users are potential targets and therefore need to be trained to properly handle unrecognized e-mails, avoid phishing tactics, and utilize basic digital-hygiene practices (e.g., strong passwords and not clicking on unknown links). Cyberattacks, such as WannaCry, serve as a wakeup call, but it is in the best interest of pharmacies to remain vigilant even when threats are not in the headlines.[7]

### 2. Build a strong relationship with your IT partner

Pharmacists can benefit from building a strong relationship with their IT partner to regularly assess the pharmacy for device vulnerabilities and implement solutions to minimize cybersecurity risks. Working closely with an IT partner to monitor systems and logs for unusual activity that might indicate an attack may help reduce exposure to cyber risks. Pharmacies should agree on the frequency of system backups with their IT partner and familiarize themselves with the process of reverting their systems back to the latest version in case of a crash.

It is strongly recommended that pharmacies

**update their software**

automatically whenever possible to ensure their devices have optimal cyber protection.

Automatic software updates should be agreed upon with an IT partner when procuring a new device or connecting a new device to pharmacy and hospital systems.

### 3. Implement cybersecurity best practices and policies within the pharmacy

To minimize cyberattack vulnerabilities, pharmacists must establish a cyber-aware culture within their organization. This can be done by ensuring all staff carry out a few simple actions such as keeping private pharmacy information off social media, not overlooking cybersecurity in general, and managing user account rights. Every pharmacy staff member does not need access to all pharmacy data, so it is important to limit access to those who truly require it. Mobile devices used in a work capacity should be heavily encrypted and have the ability to be wiped remotely in case of theft.

Pharmacies should implement
**a policy to control access to removable media**
(e.g., USB sticks containing pharmacy data).

Risks of USB usage include the potential exposure of sensitive data if lost, as well as infected USB sticks introducing malware to pharmacy networks. Pharmacies should consider controlling the use of USB ports on devices to mitigate the risk of cyberattacks.[20]

### 4. Be prepared for cyberattacks to ensure continuation of pharmacy services

Cyberattacks have become increasingly frequent and consequential in recent years, therefore pharmacies should prepare an incident response and business continuity plan.

Incident response and business continuity plans should be
**regularly tested and stored offline.**[20]

Additionally, collaboration with manufacturers may allow facilities to better monitor new alerts to keep up with critical or urgent patches and updates.

## 5. Ask suppliers the right questions when buying new connected devices

The FDA has published guidance on cybersecurity in medical devices for manufacturers.[21]

This guidance recommends:

- preparing a list of all cybersecurity risks that were considered in the design and development of a new device and a corresponding list of controls that were implemented to address those risks
- including cybersecurity controls applicable to a device's intended use in their user instructions
- monitoring for, identifying, and addressing cybersecurity vulnerabilities as a routine part of their post-market management of medical devices

### Questions for new medical device suppliers

How is data on the device protected?

How is data that is transferred to or from the device protected?

What features does the device incorporate that may protect against cyberattacks?

How were the device's cybersecurity features validated?

Has the device received cybersecurity certifications by any governing bodies or independent entities?

Underwriters Laboratories (UL), a global safety consulting and certification company, developed a series of FDA-recognized verifiable criteria for assessing the cyber vulnerability of network-connectable products and systems. Applicable to a broad range of interconnected devices, the UL 2900 series - Standard for Software Cybersecurity for Network-Connectable Devices - addresses software vulnerabilities and weaknesses and provides a universal standard for validating the cybersecurity protection of medical devices against known malware.[22]

The UL 2900 standards include requirements specifically for medical and healthcare systems (UL 2900-2-1).[22]

Products with UL 2900-2-1 certification have **undergone extensive testing** by an independent third party and have provided evidence for actions taken to mitigate potential cyberthreats.

The standards provide medical device manufacturers with a method for demonstrating their efforts to mitigate cyberattacks against their products, as well as maintain the safety and security of patients and their medical data.

## Conclusion

Building the cyber resilience of a hospital is vital and a shared responsibility.

Decision makers should enforce the proper policies and consider cybersecurity in purchasing decisions, and manufacturers should equip their products with the appropriate cybersecurity measures. With new cybersecurity standards like UL-2900-2-1 becoming increasingly adopted, the industry is taking the necessary steps to mitigate the risk and likelihood of future cyberattacks.

Cybersecurity is a matter of compromise. Utility and safety need to be balanced with security and privacy, especially in a life-critical environment such as precision medicine. A physician who wants to store or access clinical data on their mobile phone is not doing so to increase exposure to cyber threats but for the sake of convenience and efficiency in the delivery of care. Similarly, an information security officer who takes a system offline to apply updates or patches does not intend to inconvenience healthcare providers, but to decrease the risks against unexpected downtime from large-scale attacks. Although striking the perfect balance between these two sides can be an arduous task and each healthcare facility will encounter its own unique set of challenges, ultimately all should ensure they have taken the necessary precautions to minimize cybersecurity risks.

**References:**

**1.** Culbertson M. Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity. Forbes. 2021. Accessed January 18 2022. https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=75a2bb80557b. **2.** Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. Reuters. 2014. Accessed January 18 2022. https://www.reuters.com/article/uscybersecurityhospitals-idUSKCN0HJ21I20140924. **3.** IBM Security. X-Force Threat Intelligence Index. 2021. **4.** HIPAA Journal Healthcare Data Breach Statistics. Accessed Janurary 18 2022. https://www.hipaajournal.com/healthcare-data-breach-statistics/ **5.** IBM. Cost of a data breach report. 2021. Accessed January 18 2022. https://www.ibm.com/downloads/cas/OJDVQGRY. **6.** Millard WB. Where Bits and Bytes Meet Flesh and Blood. Ann Emerg Med. 2017;70(3):17-21. **7.** Ehrenfeld JM. WannaCry, Cybersecurity and Health Information Technology: A Time to Act. J Med Syst. 2017;41(7):104. **8.** Sir Amyas Morse KCB. Investigation: WannaCry cyber attack and the NHS: Report by the Comptroller and Auditor General. National Audit Office. 2018:1-31. **9.** Cyber Security Policy. Securing cyber resilience in health and care. Department of Health & Social Care. 2018:1-21. **10.** European Union Agency for Cybersecurity. SMART Hospitals: security and resilience for smart health service and infrastructures. ENISA.2016:1-56. **11.** Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices (Auckl). 2015;8:305-316. **12.** Argaw ST, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020;20(1):1-10. **13.** Moses V, Korah I. Lack of security of networked medical equipment in radiology. Am J Roentgenol. 2015;204:343–53. **14.** FDA News Release, January 15, 2016. https://www.fda.gov/news-events/press-announcements/fda-outlines-cybersecurity-recommendations-medical-device-manufacturers. Accessed Mar 28, 2022. **15.** Software as a Medical Device Working Group. Software as a Medical Device: Clinical Evaluation Guidance for Industry and Food and Drug Administration Staff. 2017:1-30. **16.** Ondiege B, et al. Exploring a New Security Framework for Remote Patient Monitoring Devices. Computers. 2017;6(11):1-122. **17.** Pycroft L, et al. Brainjacking: Implant Security Issues in Invasive Neuromodulation. World Neurosurg. 2016;92:454-462. **18.** The Center for Internet Security. The CIS Critical security controls for effective cyber defense. 2016:1-92. **19.** The US Department of Health and Human Service. Cybersecurity: The protection of data and systems in networks that connect to the Internet - 10 Best Practices for the Small Healthcare Environment. 2010:1-44. **20.** Australian Cyber Security Centre. Strategies to Mitigate Cyber Security Incidents – Mitigation Details. 2017:1-47. **21.** Center for Devices and Radiological Health, U.S. Food and Drug Administration. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. 2014:1-9. **22.** Underwriters Laboratories. Cybersecurity of Medical Devices and UL 2900. 2016: 1-11.

Baxter Healthcare Corporation
One Baxter Parkway / Deerfield, Illinois 60015
Tel.: 224.948.2000