Saisystems TECHNOLOGY

# From the Saisystems Technology Blog

## Cybersecurity Hygiene is a Priority, Even During COVID-19

### Key cybersecurity statistic warns about upcoming threats

The Secretary of U.S. Department of Health and Human Services (HHS) Breach of Unsecured Protected Health Information reported 592 breaches of unsecured protected health information, 306 of which was submitted in 2020. On top of that, healthcare is predicted to suffer from 2x to 3x more cyberattacks in 2021 than the average number for any other industry.

These numbers paint a grim picture for cybersecurity in healthcare: emerging threats, low awareness, and increasing stress on cybersecurity hygiene.

### What is cybersecurity hygiene?

Think of cybersecurity hygiene as your immune system: it protects you from viruses and other external threats. Just as you need frequent exercises to keep your immune system healthy, your cybersecurity requires the same care and maintenance to perform at its best. Bad habits and negligence can weaken your systems and expose you to harmful viruses.

Keeping your cybersecurity hygiene is an on-going effort that includes regular testing, updates and maintenance to ward of both natural deterioration and external threats. Maintaining good cybersecurity hygiene requires the active participation of both system administrators and end-users, with the latter taking a more and more critical role in ensuring your online security.

### Big impacts, low awareness

Stolen credit card and bank account numbers are the most well-known type of security breach. However, healthcare information is even more valuable in the black market than financial data. Stolen healthcare information can reveal anything from the patient's confidential health information, credit card numbers, bank account numbers, Social Security numbers to intellectual property related to medical study and inventions. This data carries significant monetary and intelligence worth to cyber thieves.

Is your systems up-to-date and capable of securing you from the latest cyber threats? Book a complimentary assessment with our team to discover potential gaps in your cybersecurity system
Data breach in healthcare, in general, leaves more damage than stolen records and violations in other sectors and industries, impacting both the providers and their patients. To put that damage into concrete numbers:

- Overall, cybersecurity breaches cost the U.S. healthcare industry over $6.45 billion, showing a 10% increase from 2019. On average, each data breach has a price tag of roughly $7 million [1]
- Hospitals spend 64% more on annual advertising following a cyberattack. This shows that breaches significantly impact patients' trust in the organization and directly impact the bottom line. [2]
- Care centers that experienced a data breach needed additional 2.7 minutes on average to deliver care to suspected heart attack patients due to delays in communication and data transfer, and saw additional 36 deaths per 10,000 heart attacks occurred annually. This shows that weakness in cybersecurity impacts organizations clinically.
- Healthcare facilities also risk legal consequences for failure in protecting their patients' privacy and sensitive information.

## Emerging threats

At the outbreak of COVID-19, many healthcare organizations quickly pivoted to telemedicine to continue providing care for patients. New technologies and applications were instrumental in mobilizing healthcare delivery and keep the population safe, but it also brought up a new challenge to many organizations: overwhelming data.

The limited timeframe to deploy telehealth solutions forced many organizations to overlook their cybersecurity foundation and its ability to support this sudden flux of data. As healthcare providers now have to carry and process more data without enhanced security, sometimes even in temporary or make-shift settings, they are more likely to face the risk of being exposed to hackers.

The pandemic also increases demand for real-time data and interconnectedness between patients and providers, and even among different providers seeing the same patient. However, the risks increase with the number of devices and people having access to your network and database. Personal devices' hacking has exploded during the pandemic due to the increasing number of patients using remote care and relying on insecure communication methods (like a cellphone).

In the face of pressing needs for changes, it is easy for healthcare organizations to sacrifice cybersecurity hygiene for convenience. Still, this sacrifice will bring significant consequences further down the road.

Technology is changing significantly and at an incredibly fast pace for both cybersecurity professionals and cyber thieves. So even with frequent preparation and systems updates, administrators always risk playing catch-up with cyberattacks and expose their data due to obsolete systems.

## Inadequate preparations

Cybersecurity has not received the attention it deserves in the healthcare industry, often under resources and priority pressure. 24% of healthcare employees in the U.S. have never received any cybersecurity awareness training [3]. 62% of healthcare administrators feel inadequately prepared to mitigate cybersecurity risks to their organizations [4].

Especially for smaller practices without a dedicated IT team or an IT professional in charge, it is even easier to overlook the need to secure your data and information. However, they are no exemption to cyber risks. In fact, a data breach might be even more detrimental and disruptive to small practices due to the high cost of clean-up and repairs, not to mention potential legal consequences.

To protect yourself against such threats, start simple: maintain a good cybersecurity hygiene. Something as simple as logging off the system when finished working may help deter a cyberattack on your organization. But don't stop at that. As you continue to grow your organizations, cyber threats also continue to evolve. Penetration testing can help you stay ahead of system exposure and proactively strengthen your defense.

Stay on top of the latest developments regarding cybersecurity threats and solutions by filling out the form below. Make sure you understand both the strengths and weaknesses of your systems. Start with regular assessments and routine maintenance of your security, and frequent examination of compliance with security regulations. Partner with a trusted vendor like Saisystems Technology for a tailored cybersecurity solution tailored to your organization's model, size and budget.

**Is your system secured? Find out now with a complimentary assessment from Saisystems Technology.**

[1] [2] [3] [4] Numbers from The 2020-2021 Healthcare Cybersecurity Report by Herjavec Group

203-929-0790 | info@tech.saisystems.com | www.saisystems.com/tech/

Saisystems TECHNOLOGY