Fighting Viruses Virtually & Onsite

Hospitals pull out all the stops to protect patients and their data

Viruses.
In breaking news and IT security briefs, they can't be escaped. Particularly during 2020 and early 2021, when nurses and IT network professionals battled viruses on two fronts: electronically and physically.

The coronavirus pandemic heightened the focus on equipment and facility sanitation, as well as makeshift treatment sites. For example, provisional wards in parking structures and pop-up negative pressure tents helped nurses treat COVID-19 patients while protecting general hospital populations.

As healthcare professionals battled the virus on the front lines, their colleagues in IT toiled behind firewalls to prevent cybercriminals from utilizing electronic viruses to steal patient health data.

Stolen healthcare records are a treasure trove of personal data, allowing them to fetch $1,000+ on the

- In 2018, approximately 15 million patient records were hacked.
- In 2019, there were 510 incidents of security breaches involving at least more than 500 records at once.
- In all, 41,335,889 patient records were exposed in 2019—196% more than in 2018!

It *Was* Yours — *Now* It's Mine
Stolen healthcare records are rich in personal information, such as Social Security numbers, wellness and mental health history, and addresses. This wealth of data allows them to command $1,000+ on the dark web. The records also enable extortion or long-term identity theft, including tax and home equity fraud that take victims years to correct (see *HealthTech Magazine*).

The federal penalties for medical record breaches can be severe, with four tiers based on three factors:

- Level of breach awareness.
- Degree of preventive action taken.
- Measures taken following any prior breach incident (view article).

Amid the ongoing COVID-19 pandemic, healthcare data attacks will likely rise once 2020's data is reviewed. Given recent history, the likely culprits behind the largest breaches will be phishing campaigns, improperly disposed files, and sophisticated cyberattacks.

How Do Breaches Occur?
For years, the suppliers of bedside equipment, such as barcode readers, have touted Internet connectivity. This setup is fast, flexible, and fairly reliable. A barcode reader is typically connected to a computer via cable or Wi-Fi. This scanning environment allows two-way communication between the device and other sources, like a server-linked PC, electronic health record (EHR) system, or an external site. Data is captured and instantly transferred upstream. Unfortunately, both Wi-Fi and Internet connectivity open the door to viruses and hackers.

1 IN 4 WIRELESS NETWORKS IS UNSECURED

Security's in the Palm of Your Hand
To help protect patients from cybercrime, advanced healthcare suppliers are fortifying devices, such as barcode readers, with:

- The Bluetooth® 5.0 wireless communication standard.
- Programming languages (e.g., JavaScript).

To understand each technology's role in securing patient data, let's review the basics of each.

Bluetooth® 5:

Worried about transmitting data via Wi-Fi? Consider a device that uses Bluetooth® 5.0 to send scanned data, e.g., from a blood bag, to a workstation running EHR software. Among their capabilities and security features, Bluetooth-enabled healthcare tools utilize cryptography, key exchange, and numeric comparison to protect data by making it harder (but not impossible) to intercept.

JavaScript platform:
Phishing scams and viruses can masquerade in 2D barcodes that a

cybercriminal may have affixed to items, such as IV bags. Once scanned, these barcodes transmit personal data to hackers. However, JavaScript programming can be loaded onto a sophisticated reader, enabling it to validate codes and ensure data integrity:

- ✅ When a 2D code is scanned, the reader can promptly analyze data and structure.
- ✅ If the match is good, the reader moves the data upstream. Bad data is deleted, and the user is alerted with five beeps.

Each of the technologies above is one part of the data security puzzle. But when combined into a healthcare-ready device, such as Code Corporation's CR2700 Barcode Reader, they form a critical line of cybercrime defense.

Coronavirus Calls for Cleanliness

As IT departments focus on preventing electronic viruses from infiltrating networks, hospital staff have been addressing the disinfection challenges that COVID-19 presents. And this is where purpose-built input devices, like the CR2700, give healthcare staff the same upper hand they give IT pros. The healthcare-ready CR2700 barcode reader features seamless construction, an IP65 rating, and CodeShield® Plastics. Particularly compelling, these

Hospitals are migrating to patient-care tools, such as barcode readers, made from disinfectant-ready plastics that withstand near-constant disinfection.

proprietary plastics withstand the chemicals found in 20 common disinfectants that degrade lesser scanners and readers. Going further, the CR2700 utilizes wireless (inductive) charging, eliminating exposed metal for additional durability against chemicals.

Don't go it alone!

In 2020, viruses taxed healthcare professionals and IT infrastructures. However, modernized input devices, like barcode readers and scanners, can help today—and in the better days ahead. These purpose-built devices will make the rounds and withstand disinfection, all while helping guard patient data.

Ready to equip frontline workers with the right weapons to fight viruses virtually and on-site?

Contact Code Corporation at info@codecorp.com or 801-495-2200 for a free demo of our purpose-built scanning solutions.