2020 MID-YEAR

# Horizon Report

THE STATE OF CYBERSECURITY IN HEALTHCARE

Fortified
HEALTH SECURITY

# CEO’s Message

We join with all of you to celebrate and applaud the selfless, brave heroes of our healthcare systems as they work tirelessly caring for people in need, protecting patient data, and reducing risk. I am confident that together we will navigate these difficult times and emerge stronger.

The COVID-19 pandemic continues to produce uncertainty, stress and disruption across all industries. Healthcare cybersecurity departments are not immune as we face unprecedented challenges as well. Cybersecurity is rooted in planning for “not if, but when” scenarios to play out. But no one could have planned for a global health crisis that transformed work environments overnight, leaving IT departments with little to no time to prepare.

> At the start of the pandemic, healthcare systems quickly realized they were either prepared to weather the storm by simply scaling their existing operations, or they needed to quickly change scope while also scaling new security initiatives.

As we move through the remaining months of 2020, periods of crisis require a renewed focus and commitment to the fundamentals of cybersecurity. Almost all of the challenges that cybersecurity teams faced pre-pandemic have remained; but with added complexity and scale. Bad actors, new and old, are now taking advantage of people’s fear and uncertainty in the chaos. Phishing emails continue to be effective in gaining access, making security awareness and training programs crucial.

We realize that many aspects of what was considered “normal,” will never be normal again. Solutions like work from home and telehealth have fundamentally changed how business is conducted, creating greater attack surfaces that must be monitored and secured.

As the financial impact takes a toll on healthcare systems’ budgets, it’s critical for security and IT leaders to demonstrate the value of each dollar spent so our colleagues can easily understand how security is, at its heart, a patient safety issue. Healthcare organizations will require more agile business operating models to truly focus on their ultimate mission of patient care and reorganize departments that would be served more efficiently through a third-party partnership.

> Almost all of the challenges that cybersecurity teams faced pre-pandemic have remained; but with added complexity and scale.

Our intent is that this Mid-Year Horizon Report builds awareness about the evolving cybersecurity landscape in healthcare and provides valuable insights for your team during this challenging time. We welcome your feedback and perspective at: *horizonreport@fortifiedhealthsecurity.com*.

Regards,

Dan L. Dodson

# 2020 Mid-Year in Review

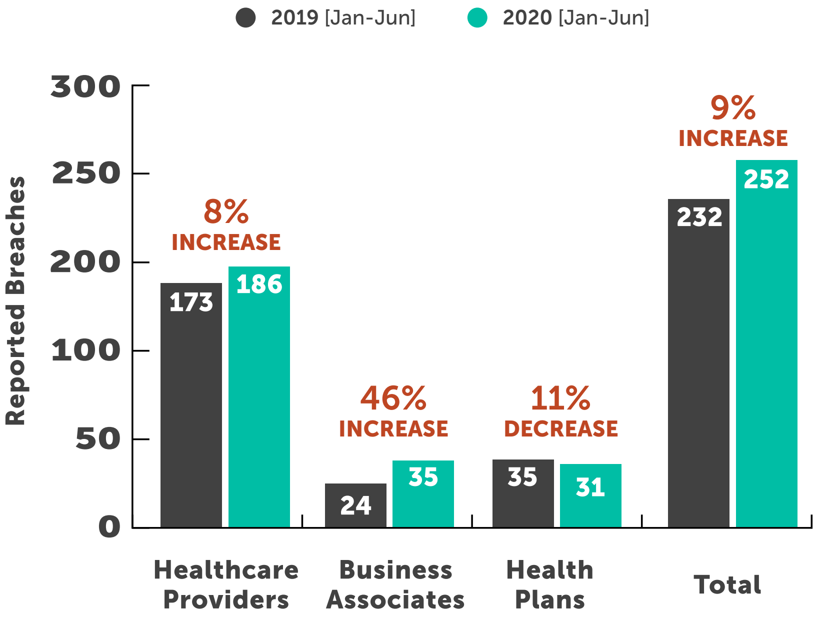
Cybercriminals continue to target the healthcare industry even as we face a worldwide health pandemic. 2020 will certainly be a year that all of us remember for COVID-19, but it also marks another year where healthcare organizations experience increased attacks from these bad actors. As healthcare organizations respond to the pandemic, our adversaries mount targeted attacks to compromise data and impact patient care, leading the FBI[1] to warn healthcare organizations and consumers that criminals are actively using COVID-19 to their advantage.

> Healthcare providers continue to be the most compromised segment in healthcare, accounting for almost 75% of reported breaches.

The exact impact of these focused attacks has yet to be fully realized, but through the first half of 2020, reported breaches increased by over 8% compared to the same period in 2019. According to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), over 253 healthcare organizations have already reported a breach this year, up from 234 for the same period in 2019.

Healthcare providers continue to be the most compromised segment in healthcare, accounting for almost 75% of reported breaches. Business associates faced a 46% increase in the number of reported breaches year-over-year, representing the largest increase of any healthcare segment. Thus far in 2020, over 5.6 million people have had their health records compromised due to these successful cyber attacks. This is down from the number of people impacted during the same period in 2019.

**Entities Involved in a Breach** [2]



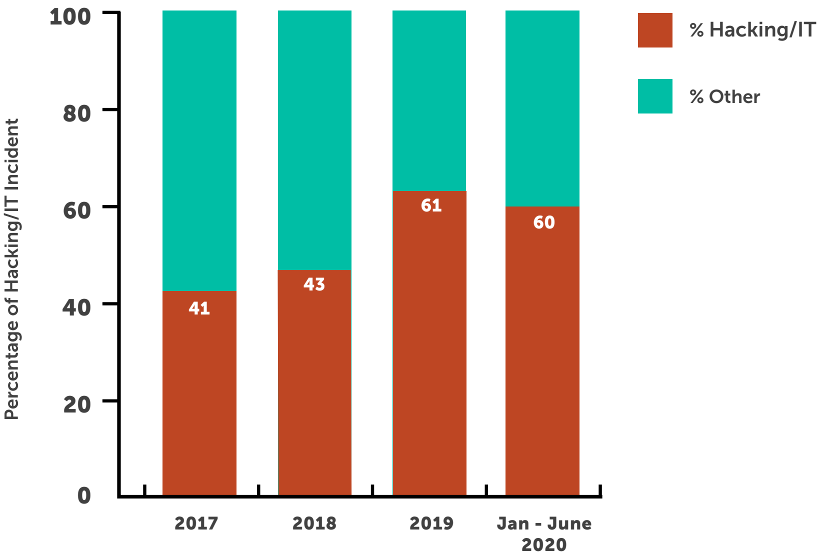
[1] Source: https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-emerging-health-care-fraud-schemes-related-to-covid-19-pandemic

[2] Source: *U.S. Department of Health and Human Services Office for Civil Rights*

A trend that has continued in 2020 is that the majority of successful attacks have been caused by malicious attackers or an IT incident. As in 2019, over 60% of reported breaches were caused by malicious attacks which have been the leading cause of breaches since 2017. As healthcare organizations respond to the sudden shift to work from home and increased adoption of telehealth, many grapple with scope and scale of their infrastructure. Safely serving patients remains the top priority of all healthcare organizations but the quick response to meet these demands may have created an increased attack surface for cybercriminals to exploit. We expect this trend to continue as bad actors capitalize on the disruption that COVID-19 is having on healthcare organizations across the world.

> As in 2019, over 60% of reported breaches were caused by malicious attacks which have been the leading cause of breaches since 2017.

While front line healthcare workers focus on serving patients during the pandemic, healthcare IT resources around the country work tirelessly to enable safe and secure work-from-home environments while scaling the availability of telehealth. These were critical activities to enable effective patient care while the world continues to react to COVID-19. Cybercriminals recognize the potential impacts these initiatives have on healthcare system employees and are significantly ramping up their phishing attacks to capitalize on this period of rapid change.



**Annual Breaches via Hacking/IT Incidents [2]**

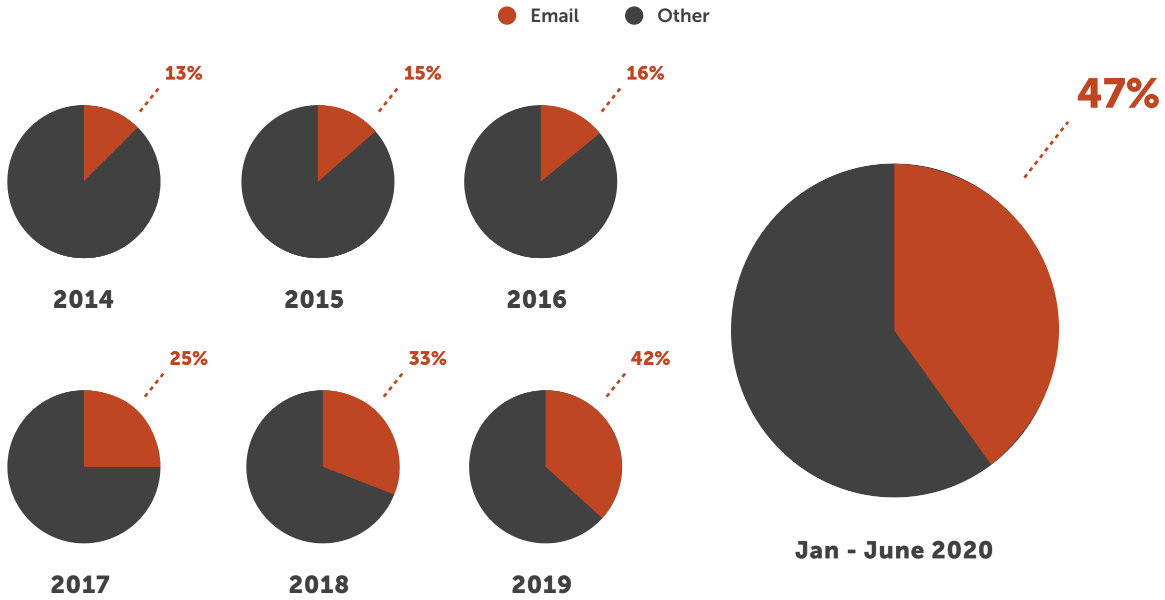
The pandemic has also contributed to the current trend of "email compromise," which remains the most common attack vector used by our adversaries to gain access to healthcare networks and steal patient data. These attacks are often executed via advanced phishing campaigns and, in 2020, bad actors are clearly leveraging the pandemic to their advantage.

[2] Source: *U.S. Department of Health and Human Services Office for Civil Rights*

Over 47% of reported breaches thus far in 2020 included email attacks, which is up from 42% in full year 2019. This is a trend we expect to continue throughout the pandemic and well into 2021. This is a stark reminder that a significant and crucial component of any strong cybersecurity program is end-user training and awareness. This is often a culture shift and requires buy-in from executive leadership within the healthcare organizations. At most organizations, getting this right can have the single greatest impact on reducing overall cybersecurity risk.

> Over 47% of reported breaches thus far in 2020 included email attacks, which is up from 42% in full year 2019.

## Annual Breaches via Email Attacks [2]



As the world adjusts to the "next normal" (whatever it evolves to), it is important for healthcare cybersecurity leaders to not lose sight of cybersecurity fundamentals. Many organizations find themselves so overwhelmed with the pandemic and looming financial uncertainty that the day-to-day execution of their cybersecurity program suffers. Healthcare organizations must continue to take a risk-based approach to managing their cybersecurity program through this pandemic because our adversaries are ramping up their efforts.

### PAUSE TO CONSIDER

1. *How has COVID-19 impacted your email security program?*
2. *Have you conducted a gap assessment to determine necessary program adjustments?*
3. *Are you executing an adequate cybersecurity training and awareness program?*

[2] Source: *U.S. Department of Health and Human Services Office for Civil Rights*

# Effects of COVID-19:
# Business as Usual vs the “Next Normal”

The COVID-19 pandemic is transforming the healthcare industry as we know it. Work from Home (WFH), changes to HIPAA regulations, and massive telehealth growth have introduced new cybersecurity challenges. And as some of your organization returns to the office, it’s important to ask: What will remain business as usual, and what will be the “next normal”?

## Transitioning to a COVID-19 Model

When the COVID-19 threat became a pandemic, organizations were required to adapt without much warning. For those who were able, this meant transitioning to a WFH model. According to April data by Gallup[3], the number of individuals who had worked remote at any point increased from 31% to 62%. This increase occurred in just two weeks. This was especially true for health systems, which historically allowed very few people to work from home. This rapid change impacted the scope and scale of cybersecurity programs for health systems.

**But what happens after the pandemic?**

As organizations are able to send employees back to a physical office, the workplace might never look the same as before. In fact, Gallup data shows that 59% of U.S. adults will opt to work remotely as much as possible if their employers gave them the choice.

Gallup data shows that 59% of U.S. adults will opt to work remotely as much as possible if their employers gave them the choice.

Many healthcare organizations’ IT and cybersecurity teams are considering allowing some associates to split time between the office and home, while some are going 100% WFH.

This data illustrates that the American workplace will look different than before, and this is especially true for the healthcare industry. The continued impact of COVID-19 has heightened the importance of cybersecurity in healthcare. From office workers managing patient data from their homes to doctors scheduling telemedicine calls, the pandemic has introduced new and broader threats to the industry.

**Many of these threats aren’t going anywhere once we return to the office.**

Organizations that fail to adjust during the transition have increased danger of potential vulnerabilities going undetected. It’s important that providers carefully plan their return to a workplace, so they can adjust to the next normal with a clear cybersecurity framework in mind.

[3] Source: https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx

# Business as Usual: What Will Remain Consistent?

From a cybersecurity perspective, there are certain factors that organizations can expect to stay the same. However, this doesn't mean that they won't require adjustments. By understanding the factors that will remain "business as usual," organizations can make decisions accordingly. Some of these factors include:

1

**Threat of Phishing Emails:** Phishing emails are among the biggest cybersecurity threats employees will face while working remotely. Remote employees may be particularly susceptible to these scams when receiving more communication electronically than ever. Malicious links can hide among legitimate emails, making them difficult to detect. These emails might look like government memos, company announcements, and messages from charitable organizations. In fact, phishing emails **tripled in number**[4] during the pandemic.

It's important that organizations understand the continued threat of phishing emails. They should be prioritizing solutions such as email encryption, link protection, attachment sandboxing, and security awareness and training. This is especially true if some of the workforce will continue to work at home all or part of the time. Consistent training and monitoring will keep these threats in check.

2

**Distraction through New Initiatives:** When your organization begins to adapt to post COVID-19 workflow, it will be tempting to launch new projects and campaigns. However, it's important to note that new initiatives can distract from executing the fundamentals. Remember that your organization's cybersecurity fundamentals are the foundation of protecting sensitive patient data.

Organizations need to continue focusing on cybersecurity basics through the post COVID-19 transition. These foundational measures can include email security, password protection, multi-factor authentication, endpoint management, vulnerability assessment and management, patching, and network monitoring. By keeping up the same diligence that your organization developed during the pandemic, you can continue to safeguard against data breaches.

3

**Talent Shortage:** Adapting to COVID-19 meant taking work, communication, and shopping online. This **increased the potential for cyberattacks**[5] globally. Factors like email phishing and malware attacks were just some of the tactics that malicious actors used to access remote networks. And the increase in attacks accelerated the demand for cybersecurity professionals worldwide.

Industry data shows that there will be **an estimated 3.5 million vacant cybersecurity positions**[6] by 2021. As your organization transitions from a fully remote model, this talent shortage will remain a concern. This is an industry-wide issue, but it may put strain on your internal IT departments. However, it's still imperative that IT teams stay on top of training and industry best practices. Some healthcare organizations are reinventing how they manage cybersecurity by forging new partnerships or leveraging talent around the world.

[4] Source: https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/

[5] Source: https://www.ncsc.gov.uk/files/Joint Advisory COVID-19 exploited by malicious cyber actors V1.pdf

[6] Source: https://www.securitymagazine.com/articles/90182-the-cybersecurity-talent-gap-an-industry-crisis

# The Next Normal: What Changes Can Your Organization Expect?

While some aspects of work will remain relatively unchanged as the healthcare industry begins to recover from the impact of COVID-19, there are some areas that will change drastically. Organizations will need to adapt to this next normal, ensuring that they're adhering to cybersecurity best practices along the way. Below are some of the most common areas that represent this transition.

**Wider Attack Areas:** As the healthcare industry adapted to the COVID-19 pandemic, telemedicine and WFH were two of the most noteworthy organizational solutions. While these solutions safeguarded patient and employee health, they also opened up more avenues for cyber attacks. Going forward, employees will likely operate from the hospital or home based on their role.

Organizations need to continue forming solutions to safeguard these workforce practices. Such solutions can include secure connections for remote employees, email encryption, advanced endpoint security, multi-factor authentication, and strict guidelines around passwords and network use. Private platforms for telemedicine calls are another key element of this security, as third-party vendor platforms may not be as secure for patients and providers.

**Third-Party Vendor Risk:** Most healthcare organizations use several third-party vendors in their day-to-day operations. These can include software for connected medical devices, as an example. Going forward, it's essential for organizations to be aware of the risks that third-party vendors can pose. Cyber attack stats from 2018 show that vulnerabilities associated with third-party vendors are behind 20% of data breaches in the healthcare industry[7]. As a result, organizations need to manage risk with third-party vendors more than ever. Failing to assess every portion of the supply chain can result in increased risk, which can be devastating post COVID-19.

**Regulatory Uncertainty:** At the beginning of the COVID-19 pandemic, the U.S. Department of Health and Human Services (HHS) and the Office of Civil Rights (OCR) loosened HIPAA rules. Specifically, they created a HIPAA limited waiver as it pertains to the Privacy Rule. This change waived the requirement for hospitals to obtain a patient's agreement to speak with family members, to request privacy restrictions, and to request confidential communications, among a list of other adjustments.

While these changes to HIPAA rules have remained for the duration of the pandemic, there is still some uncertainty if the government will uphold or reverse the waiver. It's imperative that organizations monitor HHS memos and remain HIPAA compliant throughout the transition.

[7] Source: https://healthitsecurity.com/news/third-party-vendors-behind-20-of-healthcare-data-breaches-in-2018

# Lessons Learned from COVID-19

Knowing what priorities will remain the same and which will be part of the next normal, organizations should make several changes to safeguard their network and data. By taking proactive steps, the healthcare industry can prevent malicious actors from taking advantage of vulnerabilities during this transition.

**Partner with Experts:** Ensuring data protection and HIPAA compliance following the COVID-19 pandemic will require professional guidance. Healthcare cybersecurity firms have great resources for assessing the state of your cybersecurity program and making adjustments accordingly. The right firm can help assess the true impact of the pandemic on your cybersecurity program and assist with a corrective action plan to minimize the real risks.

**Provide Employee Training:** Your employees are on the front lines of cybersecurity. Whether they're working in the hospital or from their home, it's critical that they have the basic knowledge necessary to spot and avoid cybersecurity threats—especially when working directly with patients or patient data. Organizations should provide thorough training and awareness on an ongoing basis, especially when transitioning to an office-remote hybrid model. This training might include best practices for email security, sensitive patient information management, and cyber emergency preparedness.

**Test Frequently and Know your Threat Surface:** Vulnerability threat management and penetration testing are key parts of any healthcare cybersecurity program. Even if in-office procedures feel more familiar, your team shouldn't relax testing protocol following COVID-19. It's essential to scan, test, know, and patch your network on a consistent basis. Monitoring is the best way to spot cyber threats before they access your network.

Also, having visibility to all external access points within your organization is key to securing the organization from the increased presence of threat actors.

**Continual Improvement for Remote Security:** Cybersecurity measures for remote employees and telemedicine will remain a top priority, even as patients begin making in-person appointments and some employees return to the office. It's likely that the modern workplace will remain partially remote long term, so keeping a strong remote security program is key. Keep in mind that this might require a larger IT staff or additional assistance from a managed IT provider.

**Know your Software:** The COVID-19 pandemic demonstrated how essential third-party software is to the healthcare industry. Telemedicine platforms, remote communication software, and file transfer platforms are just some of the ways that third parties support the delivery of patient care and support your employees. Organizations need to understand in great detail the configurations and content of the protocols in use for software within their environments and update as necessary. This includes communicating with third-party vendors about security concerns, which can help you understand the backend of the software. Don't forget to assess any new software that you may have implemented during the pandemic that might have slipped through your normal third-party risk governance program.

### PAUSE TO CONSIDER

1. *Did you have cybersecurity initiatives that needed to be scoped and scaled during the pandemic?*
2. *How much risk did you accept when quickly onboarding new third-party vendors during this time?*
3. *Do you conduct regular risk assessments to identify risks and document your risk management plan?*

# Work from Home: Guidelines for Remote Security Awareness

If there is anything that the first half of 2020 has shown, it's the value of working from home. The ability to adapt to a remote model has been key to employee health during the COVID-19 pandemic. However, dispersed workplaces have also presented new cybersecurity challenges within the healthcare industry. By maintaining cybersecurity awareness and best practices, organizations can stay ahead of cyber threats while employees continue to work remotely, even after the pandemic.

## Security Best Practices for Remote Work

Estimates show that 56% of jobs in the United States[8] are at least partially compatible with a remote work model. However, many jobs currently remain in-office. COVID-19 presented a new challenge to the workforce: Get as many employees working from home as possible. And this meant quickly adapting to new cybersecurity best practices.

1 **Prioritize Email Security:** Phishing is one of the top methods that cybercriminals use to gain access to networks and sensitive data—and incidences of these scams can increase when employees work remotely. This is likely because remote work relies heavily on email – i.e. rather than attending a team meeting for updates, employees receive email memos. Unfortunately, malicious actors may disguise a phishing email as a legitimate email from an employer, government agency, or other organization. Organizations need to prioritize strong email encryption and train employees to spot phishing scams. Doing so can help prevent major losses from accidental data breaches.

2 **Develop a Network Security Plan:** When an organization is working remotely, every employee is on a different network. This drastically increases the number of potential entry points for hackers. It can be wise for organizations to implement a secure remote access solution for employees. But if workers are using private networks, they should be trained on network security best practices (like setting up strong passwords). This keeps data like sensitive patient information and company financial reports safe from malicious actors.

3 **Enhance Identity & Access Management:** As our workforce has migrated to remote work, they usually rely on one thing to gain access to resources, their credentials. During this heightened period of uncertainty and remote access needs, it makes perfect sense to perform a review of access for all personnel to ensure they have the minimum access necessary (least privilege access) to perform their jobs. Ensuring you have a programmatic password management strategy and removing excessive permissions or even stale and stagnant accounts, reduces the threat surface area of the healthcare organization. Performing increased reviews of system access and monitoring for unusual access are key to identifying potential incidents and managing risk from external threat actors.

[8] Source: https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

4. **Maintain Network Access Control (NAC):** When employees work from home, they should maintain the same level of access as they would while working in the office. So, if you're operating by the principle of least privilege (POLP), each remote employee would have the minimum amount of access necessary to data, dashboards, and third-party programs to complete their day-to-day responsibilities. Network access points and margin for human error are minimized when each employee has minimal network access. Measures such as security policy checks, security posture verification for devices connecting to the network, and blocking non-compliant devices should be heavily considered.

5. **Set Up Multi-Factor Authentication (MFA):** Passwords aren't enough to protect sensitive company information. Weak or duplicate passwords can be an open door for cybercriminals. Additional layers of security are a must. MFA when using external facing resources can dramatically reduce vulnerability to malicious activity like password guessing. If MFA isn't an option, single sign-on is a login method that can make it easier for IT departments to monitor user activity and cut down on the number of weak passwords and entry points.

6. **Ensure Data Encryption:** Your team sends information back and forth all day while working remotely. And that data can be dangerous in the wrong hands. However, data that's encrypted will minimize risks associated with hackers. Even if they did obtain it, encrypted data is useless without the encryption key. Your cybersecurity team needs to be extra diligent about encryption when any employees are working remotely.

7. **Consider Alternative Models:** IT and cybersecurity teams are already stretched thin, and remote work has presented new challenges for every industry. Now may be the right time to partner with a cybersecurity managed services company. Cybersecurity firms are up to date on the latest threat intelligence and can provide additional bandwidth for monitoring and management elements of your cybersecurity program.

While remote work looks different for every healthcare organization, cybersecurity should be a priority across the board. It's essential to communicate closely with employees, ensure your security program remains a priority, and execute plans to ensure your companies boundaries are safe. This may include penetration tests to identify vulnerabilities to your internet-facing services to maintain data protection. Organizations should also carefully track industry trends and government memos that indicate prevalent threats and security best practices.

While remote work looks different for every healthcare organization, cybersecurity should be a priority across the board.

# Challenges with a Hybrid Model

As organizations adapt to network security best practices for remote workers, an important question remains:

**What if your employees spend some days in the office and some at home?**

A hybrid work model will likely become the next normal for many hospitals, so organizations need to stay ahead of the curve in order for their cybersecurity frameworks to protect them. It's important to remember that employees working in multiple locations expand the scope of your company network. You'll need to continue remote cybersecurity best practices, while also keeping up with security needs in the office, which may require additional resources.

The hybrid model presents an additional opportunity to outsource part, if not all, of your cybersecurity tasks. For example, you might hire a cybersecurity company for penetration testing and periodic compliance audits. Some organizations will benefit from managed services, where monitoring the threat and vulnerability landscape or Security Information and Event Management (SIEM) may be best managed by a third party.

No matter the approach you choose, be sure to continue monitoring, testing, and patching your environment. Treating in-office and remote threats equally will promote companywide security and compliance.

Human error causes
90% of data breaches[9].

## Security Awareness Programs

While every organization should have strong data loss prevention techniques and policies, actual day-to-day cybersecurity is only as effective as the employees and their knowledge of basic cybersecurity principles. Human error causes 90% of data breaches[9]. All it takes is a malicious link, weak password, or unsecured home network or public access point for a data breach to occur.

With this in mind, every organization needs to create and follow through on a robust security awareness and training program for remote and in-office employees. This training program might include focus areas such as:

**Device Guidelines:** If employees are using company computers at home, they'll likely benefit from secure use guidelines. These guidelines can include limits on downloading apps and programs. You should also inform your employees if your IT department will be monitoring their devices for any dangerous activity. This training should include mobile device guidelines as well, if relevant. All employees should know to log out of devices and shut them off when not in use.

**Software Management:** Even if your IT department installs antivirus and anti-malware programs on employee devices, it may be up to the employees to keep them up to date. Otherwise, the programs may not be as effective. Provide guidelines on how to keep up with software patches through updates. Employees should also know who to contact if they suspect that their computer has been compromised. Asset management is also crucial in a remote work environment.

[9] Source: https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error

**Email Best Practices:** Since remote work can increase risk for email phishing scams, employees need to be trained on how to spot malicious links and attachments. They should also be wary of file attachments from unknown senders or any sender outside of your organization. If your IT team knows of any common phishing scams circulating in your industry, be sure to notify your employees via regular security awareness communications.

**Web Browser Guidelines:** Employees may be more likely to browse the internet while working from home, which can present additional cybersecurity risks. It's important that employees know how to identify secure and trusted URLs. Web browser training should also instruct employees to avoid downloading files from unknown sites, update their browser, and avoid third-party browser plugins.

**Offline Training:** When it comes to cybersecurity, we often focus on the applications and activity on computers and mobile devices. However, a simple piece of paper left on a desk can also be a cyber threat. Organizations should remind employees to keep paperwork with company information out of public view.

**Emergency Preparedness:** Prevention training is a key part of any security program, but employees should also be aware of what to do in the event of a potential security incident. Train employees on who to contact and what actions to take if they believe that their device has been compromised. Through this early action, your cybersecurity team will have an opportunity to address the threat more quickly. Employees should also be trained to execute their Incident Response Plans from remote work locations.

Healthcare organizations should hold frequent training sessions on security awareness, especially when employees are working remotely. IT and cybersecurity teams might hold training when you notice a common issue, receive a memo about a cyber threat in your industry, or start using a new program. The key is to keep employees in the loop, so they can avoid common errors and security pitfalls.

As healthcare organizations cope with the effects of the COVID-19 pandemic, IT departments are likely feeling the strain. A remote or hybrid workforce presents a wider spectrum of cybersecurity threats. By developing clear best practices for remote work and proactively managing their security programs, healthcare organizations can safeguard their networks from malicious actors. And of course, healthcare cybersecurity companies can assist you in prioritizing network vulnerabilities, mitigating risks, and safeguarding sensitive patient information.

## PAUSE TO CONSIDER

1. *Will you continue to work from home or have some sort of hybrid work from home model in perpetuity?*
2. *Do you implement the principle of least privilege access on your network?*
3. *Do you conduct security and awareness training for your remote workers?*

# Telemedicine: Looking Toward the Unknown Future of Healthcare

Due to the risks and challenges of in-office healthcare posed by this year's COVID-19 crisis, telemedicine has become an increasingly required and popular option across America and the world. With people recommended to stay home and limit contact, many non-emergency clinicians are seeking alternative ways and methods of connecting with patients. Telemedicine, which uses technology to bridge the physical gap between patient and provider, is proving to be critical in continuing patient care. All sectors of medical service, from mental health, to dermatology, to general practitioners, have incorporated telemedicine into their practices in some form or another, with the field growing exponentially over the past few months.

## Defining Telemedicine and Telehealth

Telehealth, as defined by HHS, is "the use of electronic information and telecommunications technologies to support and promote long-distance clinical healthcare, patient and professional health-related education, public health and health administration." These technologies can take multiple forms, such as videoconferencing, store-and-forward imaging, streaming media, and wireless and terrestrial communications.

The use of the term "telemedicine" has gained traction over the last few years as the healthcare industry continues to adopt digital solutions. Telehealth and telemedicine, while often used interchangeably, should be considered as separate terms. While telemedicine is not always specifically defined by governing healthcare agencies, an increasing amount of organizations are drawing a distinction between the two.

According to the ONC, telehealth is different from telemedicine[10] because it refers to a broader scope of remote healthcare services than telemedicine. While telemedicine refers specifically to remote clinical services, telehealth can refer to remote non-clinical services, such as provider training, administrative meetings, and continuing medical education, in addition to clinical services.

Telemedicine should be the primary focus of your security program under these definitions, since it pertains directly to electronic Protected Health Information (ePHI).

These technologies allow patient/provider interaction in a safe, no-contact environment. But the ease of which patients can now receive care does not come without costs. Security risks associated with telemedicine are many and varied.

## Multiple Telemedicine Platforms

The implementation of telemedicine programs is just as diverse and requires many different platforms. Because there is such a breadth of scope for practitioners, there is not a "one-size-fits-all" single telemedicine platform that is used across the board. In fact, many health systems report using multiple platforms to deliver virtual care within the same health system, as different providers have varying needs and capabilities.

Although usage has dramatically increased in the last quarter, the telehealth field is fairly well-established and has been growing organically in recent years. Examples of traditional telehealth software companies include American Well, Synzi, Teladoc Health and Zipnosis.

[10] Source: https://www.healthit.gov/faq/what-telehealth-how-telehealth-different-telemedicine

These platforms allow doctors to consult with, educate, and in some cases, diagnose patients from the comfort and safety of their own homes. As programs developed for the medical community, they were created with healthcare-specific information security in mind.

Due to our current crisis situation, however, many health practitioners have had to quickly seek new ways to reach patients beyond these tried and true platforms. Without much notice, healthcare systems were forced to innovate and implement new forms of communication. Consequently, lawmakers have been forced to adapt by relaxing regulations regarding healthcare organizations' telehealth solutions.

The OCR announced on March 18th that it would not be imposing penalties for HIPAA noncompliance towards providers utilizing telehealth platforms that might not adhere to privacy regulations during the pandemic[11]. This relaxation relies on practitioners operating in good faith that best practices are being followed.

According to HHS, a covered healthcare provider that wants to use audio and/or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency, can use any non-public facing remote communication product that is available to communicate with patients. (Non-public facing meaning communications that are not broadcast or shared with the general public, as opposed to, for example, Facebook Live or TikTok.) Because of this, in addition to well-respected telehealth software, relaxed guidelines have now allowed for provider and patient communication to occur in private, non-HIPAA compliant platforms.

These programs are often free and easy to implement, along with being more familiar to the average patient and physician. Of course, these software programs were not designed for use in the healthcare sector and present many additional security challenges.

A provider which initially lacked end-to-end encryption for instance, made headlines in recent months for a proliferation of malicious attackers / digital vandals impacting meetings on their platforms. This potentially exposes patient health information to theft and misuse.

To combat this, purpose-built features provided by some industry platforms offer higher levels of security for medical clients and claim to be HIPAA-compliant.

These medical users have different account settings than the general public, and many features are disabled such as cloud recording, meeting chats and file sharing. Participant identities are also not reported or logged. Still, this medical-use feature is nowhere near as secure as traditional healthcare software would be.

Another challenge of these programs is that patients use them on their personal computers or mobile devices, where internet browsers may be open, or other non-secure applications are running. And on the provider side, more clinicians are working from home or on their own networks and devices, which can pose even greater security threats.

## Associated HIPAA Risks

Even with traditional telehealth platforms, HIPAA risks are very real. Telemedicine-specific HIPAA guidelines are contained within the HIPAA Security Rule and state:

- Only authorized users should have access to ePHI;
- A system of secure communication should be implemented to protect the integrity of ePHI; and
- A system of monitoring communications containing ePHI should be implemented to prevent accidental or malicious breaches.

In order to comply with HIPAA regulations, telehealth providers have flexibility in selecting their safeguards. Some potential methods for preventing confidential information from being breached include secure peer-to-peer network connections, log management solutions, intrusion detection systems, and client-side data encryption.

Still, hacking is always an issue when working in these programs. Many malicious attackers have taken advantage of the pandemic and broader use of communication software.

[11] Source: https://healthitsecurity.com/news/ocr-lifts-hipaa-penalties-for-telehealth-use-during-covid-19

Of course, there are practical steps healthcare systems and providers can take to mitigate some of these risks, including:

- Any patient materials used in remote work should be kept in a secure, designated area;
- Confidential ePHI should be accessed only through an internal network or cloud-hosted records system;
- Never store or copy protected health information on personal devices;
- Keep provider-patient communications at a low volume and only in private areas (don't use speaker features);
- Avoid using public WiFi in favor of encrypted wireless communication;
- Discourage use of shared devices;
- Utilize unique individual identities and not generic logins; and
- Prohibit use of non-approved software or applications for transmitting or communicating patient information.

By maintaining these standards, risks can be minimized but they are never eradicated.

## Will Restructuring to Telemedicine Cannibalize Business?

Another consequence of this restructuring to out-of-office care is a potential for reduced insurance reimbursement. It is unclear whether insurance companies will reimburse at the same rates for telemedicine as they have for in-office care. Conducting virtual visits may keep a health system in business and allow for necessary patient assessments for treatment but may not be conducive to long-term sustainability. Although services are still being rendered, they may not require the same physical locations or even the same amount of support staff, while rent and other selling, general and administrative expenses still persist.

> The long-term consequences of telemedicine for the healthcare industry remain to be seen.

Some health systems are have already begun restructuring in response to the changes brought on by telemedicine. Systems that are embracing telehealth and other means of virtual healthcare may close physical locations or limit service and reduce staff as they become effectively redundant. Leadership changes are another potential side effect, as manager roles could shift and the number of supervisors might be reduced based on much-decreased foot traffic.

The long-term consequences of telemedicine for the healthcare industry remain to be seen. Like it or not, healthcare is still largely fee for service and most health systems operated on tight margins pre-pandemic. Therefore, a major factor on how prevalent telemedicine is going forward directly relies on how virtual care will be reimbursed. While the landscape is rapidly changing, new and diverse challenges will continue to arise.

### PAUSE TO CONSIDER

1. *Did you have a telemedicine platform in place pre-COVID or did you have to scope and scale a new system?*
2. *Did you bypass governance plans to establish a telemedicine program? What have you had to do to address this after the fact?*
3. *Are you monitoring the platform provider to ensure they are meeting HIPAA requirements?*

## HEALTHCARE'S CYBERSECURITY PARTNER®

### INQUIRIES

1 (615) 600-4002
*horizonreport@fortifiedhealthsecurity.com*

### OFFICE

2550 Meridian Blvd, Suite 190
Franklin, TN 37067
*fortifiedhealthsecurity.com*

### FOLLOW US

### ABOUT FORTIFIED HEALTH SECURITY

Fortified Health Security is healthcare's recognized leader in cybersecurity – protecting patient data and reducing risk throughout the Fortified healthcare ecosystem. As a managed security service provider, Fortified works alongside healthcare organizations to build tailored programs designed to leverage their prior security investments and current processes while implementing new solutions that reduce risk and increase their security posture over time. Fortified's high-touch engagements and customized recommendations provide ROI and result in actionable information to reduce the risk of cyber events. The company is 100% committed to creating a stronger healthcare landscape that benefits more clients, protects more patient data, and reduces more risk.

## ABOUT THE AUTHORS

**Dan L. Dodson** serves as CEO of Fortified Health Security, a recognized leader in cybersecurity that is 100% focused on serving the healthcare market. Through Dan's leadership, Fortified partners with healthcare organizations to effectively develop the best path forward for their security program based on their unique needs and challenges.

Previously, Dan served as Executive Vice President for Santa Rosa Consulting, a healthcare-focused IT consulting firm, where he led various business units including sales for the organization. He also served as Global Healthcare Strategy Lead for Dell Services (formally Perot Systems), where he was responsible for strategy, business planning and M&A initiatives for the company's healthcare services business unit. Dan also held positions within other healthcare and insurance organizations including Covenant Health System, The Parker Group and Hooper Holmes.

Dan is a thought leader in healthcare cybersecurity and is a featured media source on a variety of topics including security best practices, data privacy strategies, as well as risk management, mitigation and certification. In 2018, Dan was recognized as a rising healthcare leader under 40 by *Becker's Hospital Review* and regularly speaks at industry-leading events and conferences including CHIME, HIMSS and HIT Summits. He also served on the Southern Methodist University Cyber Security Advisory Board.

Dan earned an M.B.A. in Health Organization Management and a B.S. in Accounting and Finance from Texas Tech University.

**William Crank** serves as Chief Operating Officer for Fortified Health Security where his responsibilities include enhancing the company's services, delivery model, and security operations center.

Prior to his role as COO, William was the chief information security officer (CISO) at MEDHOST. He has decades of information technology and security experience that include managing the Information Security Risk Management (ISRM) team at Hospital Corporation of America (HCA), where he led a team of Information Security professionals who managed compliance and information security risk and developed and implemented an operational risk management model.

William retired after serving 20+ years from the United States Navy. He currently holds multiple certifications in the areas of Information Security and Information Technology.