**Telehealth and Cybersecurity:**

**Is Your Crisis Solution Putting You at Risk?**

Name two dominant influences on 21st century healthcare and it’s a safe bet that telemedicine and cybersecurity would make the list. In the last 20 years, telemedicine has radically cut healthcare costs and [brought life-saving care into rural and underserved areas](https://globalmed.com/covid-19-a-catalyst-of-change-for-rural-america/); during the same period, cybercrime has boomed, with attackers repeatedly targeting healthcare organizations’ rich stores of valuable data. The [black market price tag of stolen protected health information (PHI)](https://www.aoa.org/news/practice-management/perfect-your-practice/healthcare-cybersecurity?sso=y) can go for $60 a record, compared to roughly $1 for a credit card or social security number.

Some providers have ignored both trends, dismissing the benefits of telemedicine while underestimating [the need for a strong cybersecurity](https://apnews.com/article/fbi-warns-ransomware-healthcare-system-548634f03e71a830811d291401651610) program. But the Covid-19 pandemic has forced nearly everyone in healthcare to reckon with both, thanks to two dynamics:

* **The rapid adoption of telehealth solutions.** In the face of a highly infectious virus, telemedicine has [stepped in like a hero](https://globalmed.com/why-did-it-take-a-pandemic-to-tell-patients-about-telemedicine/), enabling remote connections to help limit contamination. More than [**41 million telehealth claims**](https://www.definitivehc.com/resources/webinars/examining-covid-driven-rise-of-telehealth-with-claims) were filed between April and July 2020, a 4,000% year-over-year increase over the same time period in 2019.
* **A sharp increase in cybercrime.** Attackers moved fast to exploit the chaos and confusion of the pandemic. [COVID-19 email scams skyrocketed 667%](https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/) just in March; more than [half a million Zoom accounts have been sold on the Dark Web](https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/). These criminals know that in the panic and fever of last spring, many providers jumped on video-only solutions such as Zoom, Mend, Doxy.me, eVisit, Teams and Skype – and skipped a thorough risk assessment, thanks to a relaxed security and reimbursement landscape. Now nervous security experts are calling these vulnerable new environments "[blood in the water](https://www.healthcareitnews.com/news/potential-security-crisis-presented-rapid-telehealth-rollouts)" to cybercriminals.

Right now, some of you may be thinking, “We’re safe; our video-only solution wasn’t HIPAA compliant at first but it definitely is now.” And it’s true that some solutions, like Zoom, took that crucial step of meeting HIPAA requirements, which is great. But cybercrime sharks are still hunting in healthcare waters – and video-only platforms are unfortunately still ripe for attack, as a recent study shows.

**Healthcare’s Insecurity Complex**

A disturbing [report from SecurityScorecard and DarkOwl](https://securityscorecard.com/resources/healthcare-industry-telehealth-cybersecurity-risks-report) names telehealth as the current biggest threat to healthcare cybersecurity. After reviewing 30,000 health organizations and the top 148 telehealth vendors, the study found increased risk across application and endpoint security, IP reputation, patching cadence and network security.

“The COVID-19 pandemic presented a multitude of juicy opportunities for bad actors,” the report noted, “ranging from phishing attempts fueled by fear of the crisis to patchy work-from-home security practices.” These opportunities led to “an [enormous increase in targeted attacks](https://www.healthcareitnews.com/news/telehealth-biggest-threat-healthcare-cybersecurity-says-report),” in part because of the speedy video solution adoption – and lack of security evaluations – so common in the early pandemic.

The repercussions of a breach extend beyond the cost of data theft and HIPAA fines for non-compliance. [Ransomware attacks have shut down entire hospitals](https://www.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html), forcing them to reroute patients to other facilities for care. Even just one incident in a private practice can frighten patients into terminating their provider relationship or avoiding virtual care in the future.

The answer? Sticking to telemedicine solutions with proven security and long-term stability. As the report authors put it, "In order for the healthcare industry to protect patient and provider data, vetting and enforcing security protocols around new technology providers remains paramount.”

That’s a reality GlobalMed has long understood, and it’s why we are the most secure telemedicine solution in the industry.

**Tested and Trusted: GlobalMed Security**

When it comes to telemedicine security, GlobalMed operates a world-class infosec program. Our people-first approach focuses not only on risk but resilience, with a robust and sustainable culture of security. Our programs include risk management, continuity of operations, incident response, vulnerability and patch management, and resiliency by design – with ongoing role-based security awareness education to keep our expertise sharp.

To ensure our customers are protected from even the latest threats, our security stack is tightly aligned to NIST and includes controls from FedRAMP, HIPAA, ISO, SOC 2 and other industry standards. When it comes to our security architecture, GlobalMed solutions protect you with:

* Strong encryption in transit and at rest
* Multi-factor authentication (MFA)
* Vulnerability scanning
* SIEM and analytics
* Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) – North and South focus
* Endpoint security, Endpoint Detection and Response (EDR), Managed Detection and Remediation (MDR), File Integrity Monitoring (FIM)
* Mobile Device Management (MDM)
* Privileged Identity Management (PIM) and Privileged Access Management (PAM) – East and West focus
* Data Loss Prevention (DLP)
* Identity and Access Management (IDAM) governance tools
* Web Application Firewalls (WAF)
* Third-party penetration testing

Finally, we live in a world of “trust but verify.” As part of our commitment to compliance, GlobalMed has these third-party attestations presently in flight:

* NIST 800-53 Rev. 5 HIGH
* SOC 2 Type II
* ISO 27001
* FedRAMP HIGH
* NIST 800-66 – HIPAA
* FDA 21 CFR Part 11 GxP

**Locking Down Protection and Power**

Earlier this year, we predicted that the COVID-19 pandemic would spark [more innovation and telemedicine adoption in healthcare.](https://globalmed.com/how-covid-19-is-changing-telemedicine-reimbursement/) That prediction came true, so here’s another one. As 2021 approaches, we still don’t know exactly how the rest of this pandemic will play out, though the latest vaccine news has been promising. But we do know that attackers will keep trying to infiltrate healthcare organizations – and we know for a fact that virtual care is here to stay. Adopting a secure telemedicine solution is the only path to protecting both patients and the healthcare organizations that care for them.