USAID
FROM THE AMERICAN PEOPLE

# Cybersecurity

## GLOBAL HEALTH

Photo Credit: Des Syafrizal for USAID

## Why Does Cybersecurity Matter for Global Health?

The global health sector is one of the most targeted industries for cyber attacks, especially as it has an immense amount of personal information in health records, while the criticality of health organizations provides leverage to ransomware attackers. The COVID-19 pandemic has only intensified the number of cyber attacks against healthcare organizations and the spread of misinformation and disinformation.

Cyber attacks have major financial implications for the global health sector, and can negatively impact patient quality of care and health outcomes when hackers restrict access to patient data or take essential services offline.A recent global survey showed that the average cost of a data breach in the healthcare industry was close to $6.45 million, meaning that healthcare organizations generally suffer costs from data breaches that are "60% higher than the cross-industry average." Patient privacy is also threatened, as medical records provide one of the most complete collections of personal information for any given individual. There is a huge global black market for these records, which are maliciously used in numerous ways, including for identity theft, blackmail, and surveillance.

### What is cybersecurity and why does it matter for international development?

As noted in USAID's Cybersecurity Primer, USAID defines cybersecurity as "*the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation.*" As USAID partner countries further their digital transformation and continue to adopt new digital tools and systems, cyber risks and vulnerabilities proliferate. Cybersecurity failures pose material threats to USAID partner countries and undermine partner country government legitimacy. USAID must protect its digital investments by ensuring that its digital programming addresses cyber harms and includes cybersecurity mitigation measures.

# Cybersecurity Trends in Global Health

Healthcare facilities collect and store large volumes of valuable data, including personally identifiable information (PII), which is a prime target for cyber attacks. As healthcare services continue to digitize and move online in the wake of the COVID-19 pandemic, they collect increasing amounts of PII from their patients. PII contained in electronic medical records is a prime target for cyber criminals, who use this data to facilitate other crimes.

Internet of Things (IoT) health devices are especially vulnerable to attacks. IoT refers to physical devices that share data with other devices using the Internet. IoT devices have proven extremely useful in global healthcare, especially during the COVID-19 pandemic. For example, relatively cheap IoT devices can help doctors monitor patients' vitalsigns remotely or facilitate telehealth services. There are also a growing number of IOT devices in hospitals and clinics. However, the design and manufacturing of many health IoT devices do not incorporate strong security, making them highly vulnerable to cyber attacks. According to one recent study, attacks against such healthcare devices were up123 percent in June 2022 compared to 2021.

Attackers increasingly use ransomware to target this valuable data. In a ransomware attack. cyber criminals block victims' access to their own data and will release it only if the victim pays a ransom. Sometimes, the criminals will threaten to release the data publicly if the ransom is not paid. Ransomware is particularly insidious in the healthcare sector because it can shut down entire facilities, preventing patients from getting lifesaving care. Attackers understand this, and use it to extort higher payments. Ransomware attacks on healthcare facilities and other global health actors have consistently increased since the 2017 WannaCry ransomware virus disrupted health services in the United Kingdom for nearly a week. Cybersecurity firm Check Point reported that in the two-month period between November 2020 and January 2021 alone there was a 45 percent increase in cyber attacks—particularly ransomware attacks—targeting healthcare organizations globally.

Cybercriminals and nation-state actors are key culprits. Though cybercriminals motivated by financial gains are the primary driver of cyber attacks in the health sector, nation-state actors also actively target healthcare organizations in both legal and illegal ways. These nation-state actors might be collecting data for cyber espionage purposes, expanding their datasets to train their own healthcare algorithms, or stealing intellectual property (IP) from medical researchers. For example, hacking collectives affiliated with Russian intelligence services are thought to have stolen COVID-19 vaccine research from vaccine developers in the United States, the United Kingdom, and Canada. This demonstrates that all health system actors—not only clinics and hospitals—require strong cyber defenses. This includes international global health NGOs, ministries of health in USAID partner countries, and USAID partners who are implementing global health projects.

Cyberattacks on health facilities are affecting patient outcomes. Not only can PII and private patient medical data be made public during a cyber incident, but cyber attacks can also put patients' lives at stake. A woman in Germany is thought to be the first documented person to die from a ransomware attack in September 2021, after her ambulance was rerouted due to a ransomware incident at the closest hospital. According to a recent survey of IT security professionals in the healthcare industry, 54 percent responded that cyber attacks against their organizations had resulted in an increase in severity of patient illnesses, and 23 percent said that these attacks had increased mortality rates.


Photo Credit: Morgana Wingard for USAID

The problem is likely worse than we think. While we have some evidence of the prevalence of cyber attacks against the global healthcare sector, much of the data on these attacks comes from higher-income countries. Due in part to less stringent reporting requirements and other factors, we have little data on cybersecurity threats against the healthcare sector in low- and middle-income countries. However, anecdotal evidence—such as the case from South Africa—and global ransomware trends strongly suggest that attacks are far more numerous than reported.

### South African hospital hack costs $3.8 million to resolve

A June 2020 cyber attack on South Africa's largest private hospital operator, Life Healthcare Group, affected its admissions systems, business processing systems, and email servers. The hospital group, which had more than 6,500 beds across 56 hospitals, was forced offline in order to contain the attack as it struggled to meet the influx of patients seeking treatment for COVID-19. While the financial impact of the attack is difficult to assess, the cost of simply restoring IT systems to full functionality was more than $4.2 million.

# Key Considerations

The following considerations present entry points for incorporating cybersecurity into global health programming:

- Understand partner country policies, strategies, and regulations around cybersecurity, data privacy, communications infrastructure, and digitalization.
  - USAID Missions and Bureaus need to understand the cybersecurity ecosystems they are operating in before designing and implementing new EEI activities. Digital Ecosystem Country Assessments (DECAs) are one mechanism for better understanding these dynamics. If your Mission does not already have a DECA, consider commissioning one.
- When using IoT devices or apps as a part of healthcare programming, ensure adequate security assessments have been conducted and plans are included for continuing to review security risks and update these devices and apps accordingly.
- Coordinate with other donors to identify areas of alignment in cybersecurity and global health.
- Design activities that support the development of resilient cybersecurity in partner countries' health systems. Also, ensure there are no cyber vulnerabilities in existing and/or completed activities.
- Identify cyber tools that can be used by partners, including the Cyber Peace Institute's Cyber 4 Healthcare project and its Cyber Peace Builders initiative.
- Embed cybersecurity considerations, resources, responsibilities, and management tools into every USAID-funded global health project.
- Develop standalone cybersecurity elements within global health projects with digital components.
- Have a clear and agreed-upon plan for how a program will respond to a cyber attack or significant data breach or compromise.

**FOR FURTHER INSIGHTS** into the cybersecurity and global health nexus in USAID programming, please reach out to USAID's Cybersecurity Team at cybersecurity.itr@usaid.gov.