DOD IG Shares Best Practices to Secure Patient Health Information

A new special report suggests that multifactor authentication, encryption and other steps can protect patients' health information.

Melissa Harris

Mon, 04/27/2020 - 11:42

Photo Credit: erhui1979/iStock

As the Defense Department continues to provide medical personnel, resources and services to the nation in its aid to the COVID-19 response, the DOD Office of Inspector General stressed that the military must continue to protect patient health information.

The office released a special report on April 23 that reviews lessons learned and best practices from previous OIG and Government Accountability Office reports to best protect "protected health information" (PHI) — a subset of personally identifiable information — from inadvertent disclosure and unauthorized access as Military Treatment Facilities ramp up national medical aid amid the pandemic.

“Because MTFs use different methods to collect patient data, such as in-person and virtual triage, continuing to exercise due diligence to protect patient data is needed now more than ever with the increased patient loads at MTFs and alternative care facilities the DOD is helping to build and operate,” OIG said.

The special report draws from GAO and DOD OIG assessments of protected health information cybersecurity from the past three years to make eight best-practice recommendations to defense health providers and cyber officials. These are to:

- Use multifactor authentication
- Create strong passwords that meet DOD length and complexity requirements
- Have MTF CIOs develop plans of action and take steps to identify and mitigate network vulnerabilities
- Encrypt data stored in defense health systems
- Limit access to information based on a user’s role in the system and write procedures for granting, elevating and deactivating user access to support limited access
- Have system administrators monitor and review activity reports for successful and failed log-ins and data exfiltration attempts
- Implement physical safeguards — such as controlled access to sensitive areas and camera surveillance equipment.

OIG stressed the importance of PHI protection amid the uptick of health care security breaches in recent years. Between April 2018 and April 2020, American medical facilities suffered 570 PHI breaches from cyberattacks, data loss, theft, improper disposal of data and unauthorized access, according to the report in citing Department of Health and Human Services findings. These breaches affected over 46 million patients.

The FBI also issued an April 1 public notice that its Internet Crime Complaint Center had received over 1,200 complaints related to COVID-19, many of which involved cyber actors that engaged in phishing campaigns against first responders, launched distributed denial of service attacks against government agencies and deployed ransomware at medical facilities.

Given recent and overall medical cybersecurity risks, OIG said that MTFs and American medical facilities overall should work to bolster their security posture.

“As medical facilities manage the increased demands associated with administering patient care during the COVID-19 pandemic, medical administrators should seek to ensure that they also identify and mitigate cybersecurity risks and threats posed by malicious actors attempting to take advantage of the Nation’s focus on caring for the sick,” OIG said. “Therefore, MTFs should ensure that they are implementing security controls to protect patient information.”

View printer friendly version
Federal Cybersecurity
MTF
Defense Department
health
COVID-19
coronavirus
Standard