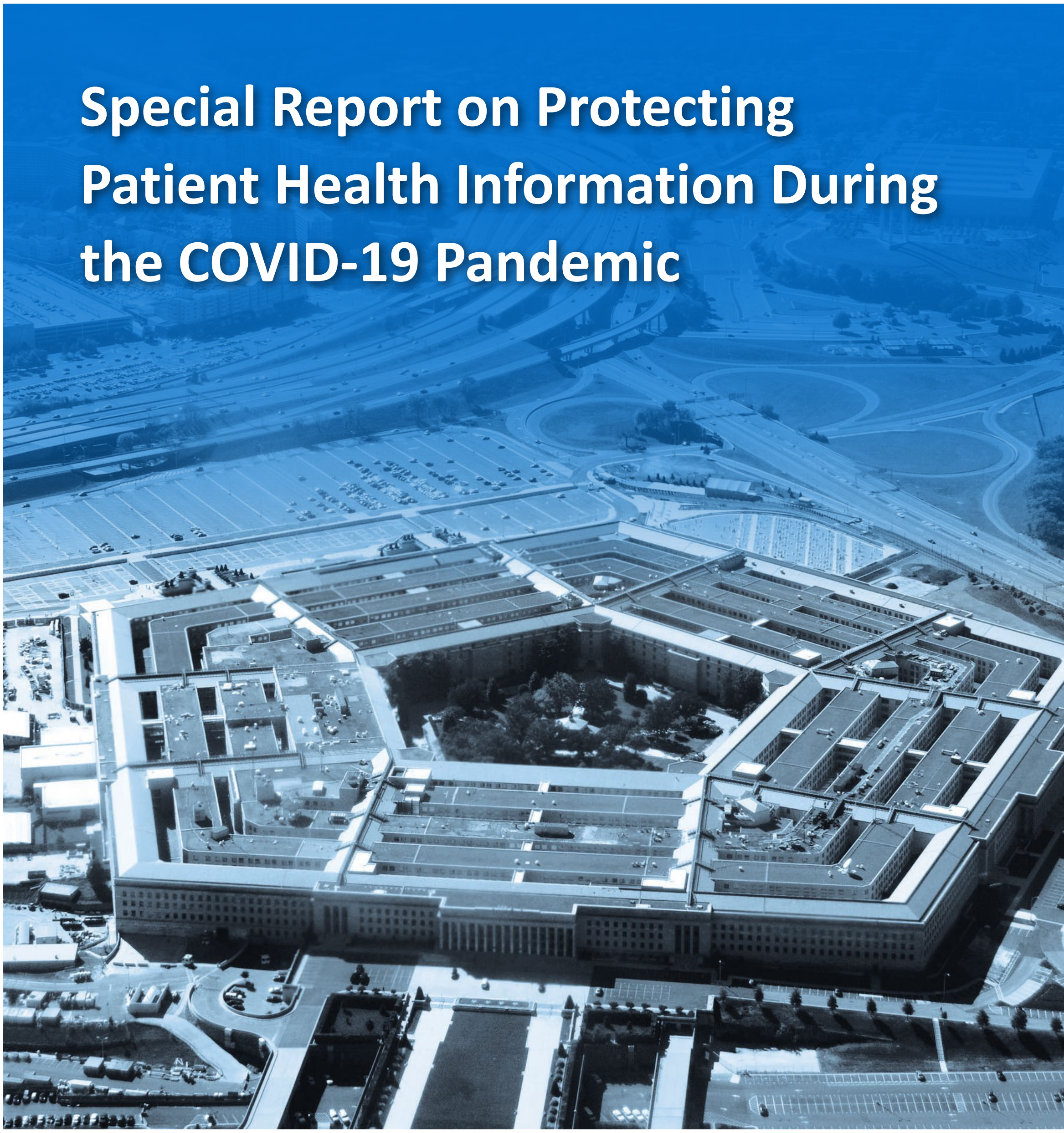
Report No. DODIG-2020-080

INSPECTOR GENERAL

U.S. Department of Defense

APRIL 23, 2020



Special Report on Protecting Patient Health Information During the COVID-19 Pandemic

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

April 23, 2020

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Report on Protecting Patient Health Information
During the COVID-19 Pandemic (Report No. DODIG-2020-080)

This special report provides lessons learned identified in audit reports related to protecting patient health information. We reviewed the following four reports issued by the DoD Office of Inspector General and the Government Accountability Office and suggested best practices for ensuring patient health information is protected from external and internal cybersecurity threats.

- GAO-18-210, “Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement,” March 6, 2018
- DODIG-2020-078, “Audit of Physical Security Controls at Department of Defense Medical Treatment Facilities,” April 6, 2020
- DODIG-2018-109, “Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities,” May 2, 2018
- DODIG-2017-085, “Protection of Electronic Patient Health Information at Army Military Treatment Facilities,” July 6, 2017

If you have any questions, please contact me at [redacted]

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cybersecurity Operations

Attachments:
As Stated

Distribution:

UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
CHIEF OF THE NATIONAL GUARD BUREAU
COMMANDER, U.S. CYBER COMMAND
COMMANDER, U.S. NORTHERN COMMAND
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS
DIRECTOR, DEFENSE HEALTH AGENCY
SURGEON GENERAL, DEPARTMENT OF THE NAVY
SURGEON GENERAL, DEPARTMENT OF THE ARMY
SURGEON GENERAL, DEPARTMENT OF THE AIR FORCE
PRESIDENT, UNIFORMED SERVICES UNIVERSITY OF HEALTH SCIENCES

CC:
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

Special Report
DoD Office of Inspector General

Protecting Patient Health Information During the COVID-19 Pandemic

On April 10, 2020, the Assistant Secretary of Defense for Health Affairs stated that military medicine is at the front lines of the national Novel Coronavirus (COVID-19) response, bringing unique and agile expertise and rapidly deployable resources to the fight. The Assistant Secretary also stated that the DoD and its Military Health System have mobilized doctors, nurses, and medical technicians from active duty and the Reserve Components to two ships and numerous expeditionary field hospitals around the country to support local health care systems. The Assistant Secretary emphasized that the DoD is diligently working to ensure that its beneficiaries have continued access to the care they need by ramping up virtual health capabilities, establishing drive-up testing sites, and putting the right protection measures in place to minimize exposure risk to patients and health care workers.

As the DoD continues to support the Nation in treating COVID-19 cases around the world, it is imperative that personnel working in military medical treatment facilities (MTFs) renew their efforts to protect controlled unclassified information, including patient health information (PHI) and personally identifiable information (PII).[1] PHI is a subset of PII, and if obtained, can be used to steal identities and reveal the health conditions and medical diagnosis of a patient. As the Nation's COVID-19 cases continue to increase and the DoD works diligently to care for the sick, the DoD must ensure that controls are in place to not only protect patients, physicians, and nurses from further spreading the virus, but also protect the sensitive and personal data collected from those individuals from unauthorized access and inadvertent disclosure. 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.

The DoD Office of Inspector General (DoD OIG) recognizes that MTFs are seeing and treating patients at increasing rates. The DoD OIG is providing this document to share lessons learned and best practices that we identified during our previous work related to the security and protection of PHI at MTFs.

[1] For the purpose of this white paper, PHI refers to patient health information. PHI is information created or obtained by a health plan or health care provider, who transmits any health information for an individual related to the past, present, or future physical or mental health or condition.

According to the U.S. Department of Health and Human Services, Office for Civil Rights, from April 16, 2018, through April 13, 2020, 570 reported health care breaches of PHI affected over 46 million patients. The Office for Civil Rights stated that the breaches occurred from cyber attacks, data loss, theft, improper disposal of data, and unauthorized access. On April 1, 2020, the Federal Bureau of Investigations issued a public advisory that cyber actors have targeted first responders and medical facilities to steal sensitive information.[2] 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. Therefore, MTFs should ensure that they are implementing security controls to protect patient information. During this COVID-19 pandemic, it is important that health care providers, chief information officers, and network and system administrators ensure that they implement security measures that decrease the risk of:

- unauthorized access to patient information;
- external threats that could exploit known system and network weaknesses; and
- internal threats to intentionally or unintentionally compromise networks and systems that contain patient information.

Lessons Learned

Over the past 3 years, the DoD OIG and Government Accountability Office (GAO) assessed the effectiveness of security controls implemented to protect DoD controlled unclassified information, including PHI and PII maintained on DoD networks and systems, from internal and external cyber threats. We reviewed four reports issued by the DoD OIG and GAO related to security weaknesses for protecting PHI.

- GAO-18-210, "Electronic Health Information: CMS Oversight of Medicare Beneficiary Data Security Needs Improvement," March 6, 2018
- DODIG-2020-078, "Audit of Physical Security Controls at Department of Defense Medical Treatment Facilities," April 6, 2020
- DODIG-2018-109, "Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities," May 2, 2018
- DODIG-2017-085, "Protection of Electronic Patient Health Information at Army Military Treatment Facilities," July 6, 2017

[2] Federal Bureau of Investigation Public Service Announcement, "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments," April 1, 2020, Alert Number I-040120-PSA.

The above-mentioned reports identified systemic weaknesses related to:

- accessing networks using multifactor authentication;
- using strong passwords that meet DoD length and complexity requirements;
- mitigating known network vulnerabilities;
- protecting PHI stored in systems or on electronic media, and data transmitted across the network;
- granting user access to PHI based on the user's assigned duties;
- configuring systems to automatically lock after 15 minutes of inactivity, except when system configurations would directly affect patient care, such as when accessing systems in operating rooms;
- reviewing system activity reports to identify unusual or suspicious activities and access; and
- implementing adequate physical security measures to protect the facilities that house PHI, including protecting electronic and paper records containing PHI from unauthorized access.

The systemic weaknesses identified increase the risk of PHI being compromised by malicious actors seeking to modify, delete, or steal sensitive information on DoD networks and systems.

Best Practices

Security protocols, such as using multifactor authentication and strong passwords, managing network vulnerabilities, and encrypting sensitive data, decrease the risk of unauthorized access to, and disclosure of, PHI. DoD and Defense Health Agency leadership, as well as system and network administrators, clinicians, and other medical personnel, should ensure that the following security protocols are in place and operating effectively.

Using Multifactor Authentication

Multifactor authentication incorporates two or more factors to achieve authentication by using something you know (password or personal identification number), something you have (cryptographic identification device), or something you are (biometric).

Using Strong Passwords

When multifactor authentication is not available, MTFs should require personnel to create strong passwords to meet DoD length and complexity requirements. According to the Defense Information Systems Agency Security Technical Implementation Guide for Network Device Management Security, passwords must be a minimum of 15 characters, including at least one upper case, one lower case, one number, and one special character.

Identifying and Mitigating Network Vulnerabilities

The MTF Chief Information Officers should develop plans of action and milestones, and take appropriate and timely steps to mitigate known network vulnerabilities. Without a rigorous and systematic process to patch vulnerabilities in a timely manner, the MTF Chief Information Officers increase their risk that cyber attacks or other malicious actions could exploit the vulnerabilities.

Encrypting Patient Health Information

Encrypting data that is stored on a system can reduce the risk that sensitive PHI can be compromised if existing security controls are breached. In addition, MTFs that download PHI on removable media should implement protection mechanisms, such as the use of encryption, to prevent unauthorized individuals from accessing information stored on removable media.

Limiting Access to Patient Health Information

Access to systems that contain PHI should be limited to those individuals with a need to know. Limiting access to PHI based on a user's role in the system that aligns with assigned duties reduces the risk of intentional and unintentional disclosure of sensitive information. Written procedures for granting, elevating, and deactivating user access increase the likelihood that only authorized users obtain access to PHI.

Configuring Systems to Lock Automatically

Medical systems containing PHI should lock automatically after 15 minutes of inactivity to limit the potential of unauthorized access to PHI, and prevent patient record manipulation, which could jeopardize patient care.

Reviewing User Activity

System administrators should consistently monitor and review activity reports for successful and failed log-ins, and data exfiltration attempts. Monitoring system activity would help to identify user and system anomalies and unauthorized access attempts.

Implementing Physical Safeguards to Protect PHI

MTFs should implement physical safeguards to protect the integrity and confidentiality of facilities that house PHI from unauthorized use and disclosure. Physical safeguards include, but are not limited to, ensuring controlled access to sensitive areas that maintain electronic and paper records containing PHI and using surveillance equipment to monitor and review access to controlled areas.

Conclusion

As MTFs and alternate care facilities experience increased volumes of patients seeking treatment during the COVID-19 pandemic, DoD health care leaders, MTF Chief Information Officers, network administrators, and users alike must be vigilant to protect the confidentiality, integrity, and availability of PHI. The Cybersecurity and Infrastructure Security Agency recommends training staff, understanding who and what is on the MTFs' network, protecting data, and minimizing vulnerabilities. Security measures, such as multifactor authentication, vulnerability management, and data encryption, decrease the risk of unauthorized access to patient information. In addition, identifying and mitigating vulnerabilities in a timely manner decreases the risk that cyber attacks could exploit known system and network weaknesses. Furthermore, limiting access to patient information to users with a mission-related need to know reduces the risk of intentional or unintentional disclosures of an individual's personal health information. Active and passive security surveillance measures, such as maintaining operating security cameras that provide the ability to monitor movement throughout a facility, also reduce the capability of insiders to intentionally compromise networks and systems that contain PHI.

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098