MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510–4606

January 16, 2020

Mr. Thomas McCaffery
Assistant Secretary of Defense for Health Affairs
Defense Health Agency
7700 Arlington Boulevard
Falls Church, VA 22042

Dear Mr. McCaffery,

As the healthcare sector becomes increasingly reliant on technology to deliver essential services to patients, it also faces rising threats from malicious actors that seek to compromise the personally identifiable and other sensitive information of Americans. As a matter of national security, the sensitive medical information of our men and women of the armed services is particularly vulnerable and should be, at a minimum, protected by robust security controls and routine scans. It is with great alarm that I recently learned that unsecured Picture and Archiving Servers (PACS) at Ft. Belvoir Medical Center, Ireland Army Health Clinic, and the Womack Army Medical Center have left personally identifiable and sensitive medical information available online for anyone with a DICOM viewer to find.

Following a report[1] in September of 2019 highlighting the exposure of sensitive medical images belonging to millions of American through unsecured PACS, I wrote letters[2] to two healthcare entities that controlled the PACS, and those images were removed. However, millions of records remained online. The following month, I wrote[3] to the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) regarding the remaining exposure of the personally identifiable information belonging to 6 million American patients. Since that letter, 16 systems, 31 million images and 1.5 million exam records were removed from the internet. However, I recently learned that a significant number of medical records belonging to servicemembers remain online. This information was discovered by the German researchers at Greenbone

[1] Cyber Resilience Report, Greenbone Networks GmbH, 2019. https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_EN.pdf
[2] Office of Senator Mark R. Warner, Warner Seeks Answers in Light of Negligent Cybersecurity Practices by Health Care Company, 2019. https://www.warner.senate.gov/public/index.cfm/2019/9/warner-seeks-answers-in-light-of-negligent-cybersecurity-practices-by-health-care-company
[3] Office of Senator Mark R. Warner, Warner Raises Alarm about HHS Failure to Act Following Exposure of Sensitive Patient Data, 2019. https://www.warner.senate.gov/public/index.cfm/2019/11/warner-raises-alarm-about-hhs-failure-to-act-following-exposure-of-sensitive-patient-data

Networks, who accessed the information using German IP addresses; this itself should have triggered alarms by the hospital information security systems.

The exposure of this information is an outrageous violation of privacy and represents a grave national security vulnerability that could be exploited by state actors or others. We owe an enormous debt to our armed forces, and at the very least, we ought to ensure that their private medical information is protected from being viewed by anyone without their express consent. Whenever data moves from one entity to another it should be protected by encryption, proper hashing, segmentation, identity and access controls, and vulnerability management capabilities that include diligent monitoring, auditing, and logging practices. To better understand how this happened, I would like information about your organization's oversight of the information security practices at military hospitals, particularly at Ft. Belvoir Medical Center and Womack Army Medical Center.

I ask that you immediately remediate this situation, and remove the vulnerable PACS from open access to the internet. To understand how these records have been exposed and accessed repeatedly by a German IP address, please also answer the following questions:

1. Please describe the information security management practices at military medical hospitals. Do you require organizations to operate on a segmented network? To implement micro-segmentation? To implement access controls? If so, what kind? Do you require the hospitals to implement multifactor authentication, logging, and monitoring?
2. Do you audit and monitor logs?
3. Do you require full-disk encryption and authentication for PACS?
4. Do you require the hospitals to have a Chief Information Security Officer?
5. Please describe what steps you took to address this issue, and when you were able to remove these systems from the internet.

Given the gravity of this issue, I would appreciate a response within two weeks.

Sincerely,

Mark R Warner

MARK R. WARNER
United States Senator