MARK R. WARNER
VIRGINIA

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

United States Senate

WASHINGTON, DC 20510–4606

November 8 2019

Mr. Roger Severino
Director, Office for Civil Rights
Department of Health and Human Services
200 Independence Ave SW
Washington, DC 20201

Dear Director Severino,

As the health care industry increasingly harnesses internet connectivity and software, including machine learning systems, to improve patient care, a long overdue focus on data privacy and information security has come into sharper focus. This is particularly evident in light of reports that sensitive medical records of potentially millions of Americans were recently exposed online – and that your agency has done little to address this issue. Prompting even greater concern, one of the companies that left the data exposed online also successfully completed one of your Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance audits in March. I am alarmed that this is happening and that your organization, with its responsibility to protect the sensitive personal medical information of the American people, has done nothing about it. As your agency aggressively pushes to permit a wider range of parties (including those not covered by HIPAA) to have access to the sensitive health information of American patients, without traditional privacy protections attaching to that information, HHS's inattention to this particular incident becomes even more troubling.

On September 17th ProPublica published a shocking report that the sensitive medical images of millions of American patients were exposed online through unsecured picture and archiving and communications servers (PACS) that utilize the Digital Imaging and Communications in medicine (DICOM), protocol.[1]The publicly-accessible information that had been accessed from Germany included MRI's, X-rays, and CT scans, as well as names and social security numbers of the patients. The 13.7 million images found on the internet required absolutely no authentication to access or download. As of writing this letter, for all U.S. territories there are 114.5 million images accessible, 22.1 million patient records, and 400,000 social security numbers, impacting an estimated 5 million patients in 22 states.[2] The largest system accessed

[1] Gillum, Jack, Kao, Jeff, Larson, Jeff. "Millions of Americans' Medical Images and Data are Available on the Internet. Anyone Can Take a Peek," September 17, 2019. https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet. The DICOM Standard is a thirteen volume set of engineering information that is used by engineers as a blueprint for the information structures and procedures that control the input and output of data from medical imaging systems. If properly designed (to the DICOM specifications), properly configured and used appropriately, equipment having a DICOM interface will communicate reliably with other DICOM equipment." https://www.ncbi.nlm.nih.gov/pmc/articles/PMC61235/. PAC servers provide storage for DICOM files.

[2] Report findings from Greenbone Networks, October 30th 2019.

holds 61 million diagnostic images attached to 1.23 million exam records of American patients and remains available on the internet.

In late August, German researchers initiated an investigation to determine the global accessibility and remote access capabilities of PACS. On September 9th, the researchers concluded their two week inquiry and submitted their findings to the German Federal Office for Information Security (BSI). By September 17th, BSI had addressed the affected systems which were removed from the internet prior to the publishing of the ProPublica report.

After US-CERT was notified of the problem by BSI, US-CERT contacted the German researchers at Greenbone Networks, confirming they received the data on September 20th. US-CERT stated the agency would convey the information to the U.S. Department of Health and Human Services (HHS).[3] According to the researchers, however, there has been no further communication from US-CERT or HHS, even though data privacy authorities from other countries like France and the UK contacted Greenbone Networks following the publication of ProPublica's report.

On September 23rd, I wrote to TridentUSA Health Services expressing my concern regarding the issues raised in the ProPublica report, and pointed out that MobilexUSA, a TridentUSA Health Services affiliate, was identified as controlling one of the unsecured PACS. On October 15th, the German researchers demonstrated to my office a number of US-based PACS have open ports, supporting unencrypted communications protocols, exposing images to the internet like chest X-rays and mammograms, and identifying details like names and social security numbers. Those images and medical records continue to be accessible.

These reports indicate egregious privacy violations and represent a serious national security issue -- the files may be altered, extracted, or used to spread malware across an organization. Earlier this year, researchers demonstrated that a design flaw in the DICOM protocol could easily allow an adversary to insert malicious code into an image file like a CT scan, without being detected.[4] The researchers who discovered the flaw in the DICOM protocol were able to use a polyglot file, which can contain more than one stream of data with different file formats, and hide the malicious code in the scan. In their current unencrypted state, CT, MRI and other diagnostic scans on the internet could be downloaded, injected with malicious code, and re-uploaded into the medical organization's system and, if capable of propagating, potentially spread laterally across the organization.

In their response to my letter, TridentUSA Health Services noted that they successfully completed the Department of Health and Human Services audits, confirming compliance with the HIPAA Security Rule, the last of which concluded in March 2019, while patient images were accessible online.

While the information security lapses by the medical companies using the PACS are clear, it is unclear how your agency has addressed this issue. As of the writing of this letter, TridentUSA

---

[3] NCCIC Incident number INC000010259928 - Medical System Exposure letter to Greenbone Networks, Sept 20th 2019.
[4] "Hacked DICOM Images Can Contain Malicious Executables," Healthcare IT Today, April 29, 2019. https://www.healthcareittoday.com/2019/04/29/hacked-dicom-images-can-contain-malicious-executables/

Health Services is not included on your breach portal website, and I have seen no evidence that, once contacted by US-CERT, you acted on that information in any meaningful way.

To understand how such an enormous oversight in your organization has allowed medical companies to leave insecure ports open to the internet and accessed repeatedly by a German IP address, I ask that you answer the following questions:

1. Did HHS receive a notice from US-CERT regarding the open PACS ports available with diagnostic imaging available on the internet without any restrictions?
    a. If so, what actions were taken to address the issue?
2. What evidence do you require organizations to produce during a HIPAA Security Rule audit? Are organizations asked to turn over their audit logs? How does OCR review the logs?
    a. Does OCR have information security experts on staff or does it rely on external consultants as part of these audits?
3. What are the follow-up procedures if an organization's log files reveal access to sensitive data from outside the United States, such as in this case?
4. Please describe your information security audit process.
5. Please describe your oversight of the DICOM protocol and PACS security. Do you require organizations to implement access controls? If so, what kind? Do you require full-disk encryption and authentication for PACS? Are the DICOM protocol implementations included in the audits?

The American people deserve to have their sensitive private information protected and their government held accountable for enforcing the rules in place to keep that information private. I hope that you will share what immediate actions you are taking, along with answering the questions above. I look forward to hearing your response no later than November 18, 2019.

Sincerely,

Mark R. Warner