Congress of the United States
Washington, DC 20515

June 27, 2016

Deven McGraw
Deputy Director for Health Information Privacy
Office of Civil Rights
U.S. Department of Health and Human Services

Dear Deputy Director McGraw,

We are writing to thank you for announcing that your office will issue guidance to help provider organizations understand how to react in the event of a ransomware attack and establish a protocol for risk assessment, response and reporting to comply with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). We also want to raise some issues that differentiate ransomware from conventional hacking and encourage the timely issuance of proposed guidance to address these differences.

According to the Ponemon Institute's Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, ransomware is one of the top three cyber threats facing healthcare organizations. More than four in ten healthcare organizations are worried about ransomware cyberattacks.

From a technical standpoint, ransomware is likely subject to a risk assessment analysis of a data breach. 45 CFR § 164.402 defines a breach as, "the acquisition, access, use, or disclosure of protected health information in a manner not permitted . . . which compromises the security or privacy of the protected health information." Ransomware typically executes itself as an encrypted lock around one or more servers, storage devices, applications or files. In order to encrypt the servers, storage devices, applications or files, the malware must access the target system or file, even in cases disabling access to particular functions involving personal health records. Since access must occur in order for any malware event that creates a disruption of service or corruption of data thereby placing patients at risk, including ransomware, the definition of a breach has been met and subject to a required risk assessment to determine what additional steps, if any are necessary.

However, just because a ransomware attack qualifies as a conventional breach, that does not mean they should be treated the same or subject to the exact same risk assessment. One reason for this difference is that the effect of a ransomware breach is different. In a

normal breach, personal health information is either viewed or stolen, infringing the privacy rights of the patient. Ransomware, however, denies access to health records or information technology functions that enable the provider to offer health care services.

In the case of a ransomware attack, the threat is not usually to privacy, but typically to operational risks to health systems and potential impacts on patient safety, and service. Ransomware that denies access to health records or functions essential to providing health care services may create a threat to the safety of the affected patient. For example, the recent ransomware attack on MedStar resulted in patients being turned away due the inability to provide care.[1] On the other hand, there may be cases where even if patient information is accessed and locked down, good data management practices such as maintaining data backups may prevent lack of access to electronic medical records or other functionality. If the provider or other party providing care would be either unable to care for the patient or unable to provide information critical to the care for the person, swift patient notification is paramount, but if the ransomware does not affect patient safety then patient notification may be unnecessary.

Therefore, we suggest that patient notification would only make sense in cases where the ransomware attack results in either a denial of access to an electronic medical record and/or loss of functionality necessary to provide medical services. In such cases, the notification should be made to affected parties without unreasonable delay following the discovery of a breach, and, if applicable, to restore the reasonable integrity of the system(s) compromised, consistent with the needs of law enforcement and any measures necessary for organization to determine the scope of the breach.

While patient notification may not make sense in every case, rapid and mandatory notification of government agencies and shared cyber-response resources is strongly encouraged. Most ransomware attacks rely on similar technology, using the same efficient but simple encryption to lock users out. In order to learn how to defeat these attacks and ensure that the attack cannot be repeated, it will be crucial to ensure both the government through the United States Computer Emergency Readiness Team (US-CERT) and healthcare based Information Sharing and Analysis Organizations (ISAOs) such as the NH-ISAC, and other private sector organizations that share cyber threat information know details about ransomware attacks as soon the information becomes available. Information sharing with DHS and applicable ISAOs also critical to enable the entire sector to develop unified responses to ransomware attacks. Therefore, we recommend guidance that aggressively

---

[1] https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html

requires reporting of ransomware attacks to HHS and appropriate health care-related ISAOs.

We also want to point out that since ransomware does not always involve viewing or stealing personal health information, requiring a provider to offer credit counseling services may be an unnecessary expense.

Finally, we urge OCR to include clear guidance related to data modification from ransomware or malware attacks, including deletion of entire servers or drives that constitute a breach under HITECH, even if the deletion does not involve direct modification of the original files. We assert that destruction of records is the same as accessing them and has a similar impact to an organization.

Thank you again for taking action on this vital issue. If you have any questions please contact Andrew Lachman in the office of Congressman Lieu at (202) 225-3976 or Andrew.Lachman@mail.house.gov or Matthew Haskins at the office of Congressman Hurd at (202) 225-4511 or Matthew.Haskins@mail.house.gov.

Sincerely,

Ted W. Lieu
Member of Congress

Will Hurd
Member of Congress

Cc: Hon. Sylvia Burwell, Secretary of Health and Human Services