MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

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

October 9, 2020

Mr. Alan B. Miller
Chairman and Chief Executive Officer
Universal Health Services, Inc.
367 S. Gulph Road
King of Prussia, PA 19406

Dear Mr. Miller:

I write you with grave concerns about United Health Services' digital medical records and clinical healthcare operations succumbing to an apparent ransomware attack. As one of the nation's largest medical facility operators with 3.5 million patient visits a year, it is imperative that medical care is provided to all patients without any interruption or disturbance created by inadequate cybersecurity. While initial reports suggest that the attackers did not access patient or employee data, an incident such as this sharply highlights the need to ensure adequate cybersecurity hygiene in a healthcare setting. The national health crisis during the COVID-19 pandemic only exacerbates the consequences of insufficient cybersecurity.

The need for health care providers to address cybersecurity threats has been obvious for several years now. Clinical providers including UHS must ensure all information, medical, and critical systems are sufficiently protected. Ransomware continues to impact organizations that have not demonstrated sufficient risk management maturity. The threat of ransomware to hospital systems – and the impact it has on clinical healthcare operations, patient care, and life safety – has been clear since 2016, when a series of major incidents occurred.[1]

Although the threats are not new, authorities have continued to sound the alarm about the cyber threats to healthcare – including the heightened impact during our current public health emergency. For example, in both countries where UHS operates, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) issued a joint alert on May 5, 2020[2]. This alert announced that advanced persistent threat (APT) groups are exploiting the COVID-19 pandemic as part of cyber operations against healthcare and essential services. Attacks observed against healthcare providers include password "spraying" attacks that automate attempts to use commonly used passwords, scanning for vulnerabilities in unpatched software, such as virtual private networks, and targeting supply chains.

[1] Kim Zetter, "Why Hospitals Are the Perfect Targets for Ransomware," WIRED, September 2016, https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets
[2] CISA Alert (AA20-126A), "APT Groups Target Healthcare and Essential Services," May 5, 2020, https://us-cert.cisa.gov/ncas/alerts/AA20126A

As UHS has expanded over four decades to encompass 250 medical facilities across the U.S., including twelve facilities in Virginia, effective clinical environment cybersecurity cannot be a casualty to value-based care cost savings and economies of scale. Indeed, hospital systems have frequently suggested to competition authorities that greater consolidation will allow for greater operational efficiencies; yet this does not appear to be the case when it pertains to something as vital as information security. An increasing number of medical facilities sharing connected information systems and computer networks requires adequate protection for a significantly larger attack surface. Any failure to protect this considerable attack surface with appropriately segmented networks and data provides opportunities for lateral movement across disparate systems. An unmitigated breach in one facility can cripple systems at hundreds of medical facilities, risking patient care throughout a large provider network while healthcare delivery remains strained by a pandemic.

With the full resources of a Fortune 500 company receiving over $11 billion in annual revenue, UHS's patients expect and deserve that their provider's cybersecurity posture to be sufficiently mature and robust to prevent major interruptions to health care operations. While UHS's latest annual report acknowledges that a cyber-attack that causes a security breach or loss of HIPAA protected health information could have a material impact on business, there is more than just business at stake when clinical operations are disrupted.

To gain a better understanding of this situation, I would appreciate answers to the following questions:

1. Please describe the UHS vulnerability management process, including your current practices relating to patch management across your health infrastructure.
2. How are various UHS facilities' networks and IT systems isolated from each other to prevent a cybersecurity breach at one facility from affecting multiple facilities?
3. Does UHS have effective segmentation measures in place within its healthcare facilities to prevent any type of malware from spreading?
4. What policies does UHS maintain relating to third-party risk management?
5. What are your cybersecurity and risk assessment requirements?
6. How are clinical medical devices isolated from administrative systems and networks to ensure a breach of the administrative network does not interrupt medical devices?
7. Who is the senior-most executive responsible for day-to-day oversight of information security and who does that executive report to?
8. Has UHS paid any ransom or does UHS plan to any ransom?
9. Have any patient medical records, HIPAA protected data, or healthcare information been affected or suffered a denial of access?
10. Have any patient medical records, HIPAA protected data, or healthcare information been exfiltrated from UHS owned or operated systems without authorization?

Patients deserve to know that healthcare systems are secure, particularly as the nation faces a pandemic straining resources nationwide. When a cybersecurity failure occurs, patients need reassurance that their healthcare provider is committed to learning from and responding to this

truly concerning incident, and that it is taking all appropriate steps to help ensure it cannot happen again.

Your response will be critical to this process, and I look forward to receiving that within the next two weeks. If you should have any questions or concerns, please contact my office.

Thank you for your attention to this important issue. I look forward to your response in the next two weeks.

Sincerely,

Mark R. Warner
United States Senator