United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510–6200

March 27, 2024

VIA ELECTRONIC TRANSMISSION

Dr. Maureen McBride
Chief Executive Officer
United Network for Organ Sharing
700 N 4th Street
Richmond, Virginia 23219

Dear Dr. McBride:

On November 10, 2023, during two software tests, the United Network for Organ Sharing (UNOS) discovered it had been exposed to a data breach as a result of a software configuration error that gave unauthorized access to at least 1.5 million patient records to Organ Procurement and Transplantation Network (OPTN) and DonorNet system users.[1] System users are authorized to view specific patient records on a case-by-case basis for the purpose of providing medical care.[2] However, system users do not have unfettered access to every patient record within the OPTN and DonorNet system, which was the result of the breach.[3] The sensitive data that was exposed included patients' dates of birth, social security numbers, and procedures.[4] Whether the exposed data was accessed by authorized users only or not, this mishandling error is another example of UNOS's failure to operate the critical technology supporting the OPTN.

Unfortunately, this is not the first time we have raised concerns regarding UNOS's inability to operate its critical technology. On January 31, 2022, we wrote to UNOS expressing concerns and asking then-CEO Brian Shepard to "[t]ake immediate action to modernize the national [OPTN]

[1] Eric Kolenich, "Organ transplant data breach grows to 1.5 million records," Richmond Times-Dispatch, January 23, 2024, https://richmond.com/news/local/business/health-care/organ-transplant-data-breach-grows-to-1-5-million-records/article_ce03f26e-b946-11ee-a19a-4f4cfee81c94.html.
[2] *Id.*; Disclosure from Patient Group Stakeholder. Emails on file with Budget Comm. Staff; *See also* Letter from Melanie Anne Egorin, PhD, Assistant Secretary for Legislation, Department of Health and Human Services, to Senators Wyden and Crapo, On File with Senate Finance Committee.
[3] *Id.*
[4] *Supra* note 1.

information technology system and secure it from cyber-attacks."[5] On February 11, 2022, we also raised concerns with the White House Chief Information Officer regarding the cybersecurity and technology used by UNOS as the nation's OPTN contractor.[6] Then, on March 20, 2023, we wrote to your organization expressing concerns about the February 15, 2023, DonorNet outage, which left patients' lives at risk.[7]

UNOS is responsible for overseeing and operating the OPTN IT System, which maintains the waitlist for all organ transplant candidates in the United States.[8] According to UNOS's website, "UNOS works for the more than 100,000 patients on the transplant waiting list to ensure they have equitable access to lifesaving organs…"[9] In 2023, UNOS facilitated more than 46,000 organ transplants.[10] Given the large amount of sensitive data UNOS stores and collects on past and present patients, it is imperative that data breaches do not happen again.

Considering our continued concerns with the security of UNOS's critical technology and its apparent inability to efficiently and effectively operate the OPTN, please answer the following questions no later than April 10, 2024:

1. Please describe how UNOS identified the existing data breach. Provide all records.[11]

2. Please describe UNOS's understanding of the root cause of the data beach and any relevant investigations or reviews. Provide all records.

---

[5] Letter from Senators Wyden and Grassley to UNOS, January 31, 2022, https://www.grassley.senate.gov/imo/media/doc/wyden_and_grassley_to_unos_-_it_security_systems.pdf.

[6] Joseph Menn and Lenny Bernstein, "Thousands of lives depend on a transplant network in need of 'vast restructuring'," The Washington Post, August 3, 2022, https://www.washingtonpost.com/health/2022/07/31/unos-transplants-kindeys-hearts-technology/. "'We request you take immediate steps to secure the national Organ Procurement and Transplantation Network system from cyber-attacks, the committee chair,' Sen. Ron Wyden (D-Ore.), and Sen. Charles E. Grassley (R-Iowa) wrote to Federal Chief Information Officer Clare Martorana in February."; Letter from Senators Wyden and Grassley to UNOS, February 11, 2022, https://www.grassley.senate.gov/imo/media/doc/wyden_and_grassley_to_omb_-_optn_tech.pdf.

[7] Letter from Senators Wyden and Grassley to UNOS, March 20, 2023, https://www.grassley.senate.gov/imo/media/doc/wyden_grassley_to_united_network_for_organ_sharing_-_donornet_outage.pdf.

[8] UNOS, *Technology for transplants*, https://unos.org/technology/technology-for-transplantation/#:~:text=Using%20DonorNet%2C%20an%20organ%20procurement%20organization%20%28OPO%29%20adds,coordinators%20whose%20casework%20requires%20traveling%20to%20different%20hospitals.

[9] UNOS, *The national organ transplant system*, https://unos.org/about/national-organ-transplant-system/#:~:text=Every%20day%2C%20UNOS%20works%20for%20the%20more%20than,or%20where%20they%20go%20for%20their%20transplant%20care.

[10] UNOS, *Actions to strengthen the U.S. organ donation and transplant system*, https://unos.org/transplant/improve-organ-donation-and-transplant-system/.

[11] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (emails, email attachments, and any other electronically created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).

3. How many patients were affected by the data breach and over what period of time? Provide all records, including any updates or revisions UNOS may have made regarding the total number of patients impacted by the data breach.

4. How many patient records were accessible during the data breach? How many patient records were actually accessed during the data breach? Provide all records, including any updates or revisions UNOS may have made regarding the total number of patient records impacted by the data breach.

5. How many, authorized or unauthorized, users were able to access patients' sensitive information during the data breach? How many actually accessed this data? Provide all records.

6. What is UNOS's process for responding to a real-time data breach or cyberattack on its technology systems? Provide all records.

7. Provide all records of communications UNOS had with HHS, HRSA, or any other federal agency in regards to the data breach.

8. Has UNOS notified the patients who had their data breached? If not, why not? Provide all records.

9. What steps has UNOS taken to mitigate future data breaches and cyberattacks? Provide all records.

Thank you for your prompt review and response. If you have any questions, please contact Tucker Akin of Senator Grassley's staff at (202) 224-0642 and Melissa Dickerson of Chairman Wyden's staff at (202) 224-4515.

Sincerely,

Ron Wyden
Chairman
Committee on Finance

Charles E. Grassley
Member
Committee on Finance