Notice of Data Privacy Incident

The United Network for Organ Sharing (UNOS) operates the Organ Procurement and Transplantation Network (OPTN) through a contract with the U.S. Department of Health and Human Services (HHS), Health Resources and Services Administration (HRSA). We are writing to share information about a data privacy incident that may have affected patient information. We take the privacy and security of this information seriously and this public notice contains information about what occurred, and steps that have been taken to remedy the issue.

What happened?

One of the services UNOS provides as part of its contract with HRSA is access to some of our information technology (IT) test environments where authorized external system developers can test and demonstrate new tools and enhancements to the OPTN system. This system is separate from the live OPTN IT system. On November 10, 2023, the UNOS IT team discovered that users of the test environments had access to confidential patient information instead of test data. Due to a process error, this information has been stored in the test environment since their creation in 2007 and 2011.

We have no indication that any users have violated our privacy policies regarding the sharing of confidential data. In addition, **we have no reason to believe any of the information was misused. There is no evidence of any malicious activity and the only individuals who had access to these environments were authorized, known users. This incident has not affected the services or care provided by transplant centers, organ procurement organizations, laboratories, and others in the transplant network.**

What information was involved?

The information present in the test environments included some combinations of Social Security numbers, dates of birth, health insurance claim numbers, the date information was added to the OPTN database, and other dates related to transplant or donor services. **The data did not contain names, addresses, financial account information or health insurance policy numbers.**

What we are doing:

Immediately after discovering the error, we took the test environments offline and began an investigation. We also hired an independent computer forensics and security experts to assist us. The experts did not find evidence that any information was exposed to the general public. Additionally, notification letters have been sent to individuals whose information was accessed by the authorized users of the test environment.

What you can do:

It is always good practice to remain vigilant for evidence of identity theft or fraud. It is important for people to review their bank account, financial statements and credit reports for suspicious activity, and promptly report any suspicious activity to your financial institution. Individuals can also visit the Federal Trade Commission's website on identity theft protection (identitytheft.gov) for information on how to place a fraud alert or security freeze on their credit file.

For more information:

If you have any questions or to find out if you were impacted by this incident, please call 1-888-598-5408, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Protecting your information and maintaining your confidence remain our top priorities.