Substitute Notice

Solventum Health Information Systems ("Solventum") is a medical technology and health sciences company that provides services for many hospital systems that involves access to and use of patient information.

What Happened?

On March 30, 2026, Solventum became aware of a data security incident that occurred on March 29, 2026, involving unauthorized access to limited systems and data related to some Solventum customers and their clients or patients. Upon learning of the incident, Solventum immediately initiated an investigation, notified law enforcement, and engaged outside forensic experts to help assess the nature and scope of the incident. They also notified impacted customers about this incident.

What Information Was Involved?

Our investigation indicated the following types of information related to patients may have been accessed without authorization: first and last name, address, dates of birth, medical record numbers, medical history and diagnoses. Please refer to the notice you received for specific details about the types of information relating to you which may have been accessed. There is no evidence that your information has been used to commit identify theft or fraud.

What Solventum is Doing

Upon discovery, Solventum took several proactive steps to contain the incident and to enhance existing security measures, including:

- Working with cybersecurity experts to investigate the circumstances behind the incident;
- Resetting compromised Solventum employee accounts;
- Rotating additional passwords and enhancing authentication controls;
- Increasing employee training related to "vishing" and other social engineering techniques;
- Tightening permission rights to sensitive information; and
- Enhancing monitoring to detect unusual login activity.

What You Can Do

We recommend that you remain alert for unusual health account activity and review any "explanation of benefits" from your health insurance provider to ensure all benefits are accurate.

For More Information

If you have any questions, please call 1-855-830-9403, or visit https://response.idx.us/solventum. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time.

We sincerely apologize for this incident and any concern it may cause you. Solventum remains committed to safeguarding sensitive information provided to it, including taking steps to bolster security measures and help prevent incidents like this from occurring in the future.

Learn More

Frequently Asked Questions

Incident Information

WHAT HAPPENED?

In late March, Solventum became aware of a data security incident that occurred on March 29, 2026, involving unauthorized access to limited systems and data related to some customers and their clients or patients. Upon learning of the incident, we immediately initiated an investigation, notified law enforcement, and engaged outside forensic experts to help assess the nature and scope of the incident.

WHO IS SOLVENTUM?

You may not recognize the name because we typically work behind the scenes with hospitals rather than directly with patients. We are a U.S. based company that provides medical technology and supplies, as well as health information systems to many hospitals systems.

HOW DID YOU RESPOND?

We acted quickly to contain the incident, reset affected accounts, enhance authentication controls, and increase monitoring. We also engaged external cybersecurity experts and notified law enforcement.

HOW WILL AFFECTED INDIVIDUALS BE NOTIFIED?

If we confirm that an individual's information was involved, we will attempt to notify them directly or through our hospital partners.

WHAT STEPS ARE BEING TAKEN TO PREVENT THIS IN THE FUTURE?

Upon discovery, Solventum took several proactive steps to contain the incident and to enhance existing security measures, including:

- Working with cybersecurity experts to investigate the circumstances behind the incident;
- Resetting compromised Solventum employee accounts;
- Rotating additional passwords and enhancing authentication controls;
- Increasing employee training related to "vishing" and other social engineering techniques;
- Tightening permission rights to sensitive information; and
- Enhancing monitoring to detect unusual login activity.

WHAT SHOULD I DO TO PROTECT MYSELF?

We recommend that you remain alert for unusual health account activity and review any "explanation of benefits" from your health insurance provider to ensure all benefits are accurate. There is no evidence that your information has been used to commit identify theft or fraud.

WHAT SHOULD I DO TO PROTECT MYSELF?

We recommend that you remain alert for unusual health account activity and review any "explanation of benefits" from your health insurance provider to ensure all benefits are accurate. There is no evidence that your information has been used to commit identify theft or fraud.

HOW DO I GET MORE INFORMATION?

If you have any questions, please call 1-855-830-9403. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time.