

May 5, 2025

*Sent Via Email at SecurityBreach@atg.wa.gov*

Office of the Attorney General  
Consumer Protection Division  
1125 Washington Street SE  
P.O. Box 40100  
Olympia, WA 98504-0100

RE: Notice of Data Security Incident

Dear Attorney General:

This letter is to provide you notice of a cybersecurity incident that we recently became aware of.

Providence Swedish was notified on March 20, 2025 of a security event at a former collections vendor, Nationwide Recovery Services, Inc. ("NRS"), affecting the patient records of Stevens Memorial Hospital, now known as Swedish Edmonds. In July 2024, NRS discovered suspicious activity related to certain systems which resulted in a network outage. NRS immediately took steps to secure their environment and launched an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access to the NRS network between July 5, 2024 and July 11, 2024, and that certain files and folders were copied from their systems. NRS worked with outside third-party specialists to assist with the investigation and incident response, and they are coordinating with federal law enforcement. NRS has implemented additional cybersecurity measures and reviewed existing security policies to further protect against similar incidents moving forward.

The compromised data accessed by the unauthorized third party includes patient names, birth dates, addresses, Social Security numbers, financial account information and/or medical-related information.

There were 746 Washington residents identified on April 21, 2025. Please find enclosed a copy of the notification that was sent to the affected individuals on May 5, 2025. Providence Swedish is offering no-cost credit services to each affected individual.

Sincerely,

Linda Liu  
Principal Compliance Consultant  
Providence St. Joseph Health  
Linda.Liu@providence.org

Providence St. Joseph Health  
P.O. Box 989728  
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

May 5, 2025

## Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

As the Chief Privacy Officer for Providence I am writing to you about a recent incident at Swedish Edmonds Hospital (formerly Stevens Memorial Hospital) located at 21601 76<sup>th</sup> Ave W, Edmonds, WA 98026 involving your personal information.

### What Happened

On March 20, 2025, Swedish Edmonds Hospital was notified by Nationwide Recovery Services, Inc. (NRS) of a security event that occurred between July 5, 2024 to July 11, 2024. The affected information was disclosed by Stevens Memorial Hospital to NRS between October 1989 and December 1997 when NRS was providing collection services for the hospital. (Currently, neither Providence nor Swedish Edmonds Hospital retains a services contract with NRS). NRS determined that between July 5, 2024 to July 11, 2024 an unauthorized third-party was able to access files and folders from the NRS network. These files and folders may have contained your personal information.

### What Information Was Involved

Specifically, the information accessed by the unauthorized third party includes your full name, date of birth, address, Social Security number, financial account information and/or medical-related information.

### What We Are Doing

**Because your information may have been compromised as a result of this incident, identity protection services through IDX are available to you at no cost for <<one year/two years>>.**

Providence has also received written assurance from NRS that once they became aware of this incident, they have confirmed the security of their systems and implemented additional cybersecurity measures.

### Next Steps

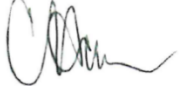
**Providence encourages you to enroll in free IDX identity protection services** at <https://app.idx.us/account-creation/protect> or by scanning the QR code or by calling 1-800-939-4170 and using the Enrollment Code provided above.

IDX representatives are available Monday through Friday, 6 a.m. - 6 p.m. Pacific Time. **Please note the enrollment deadline for free IDX identity protection is August 5, 2025.**

**For More Information**

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the Enrollment Code at the top of this letter when enrolling, so please do not discard this letter.

Sincerely,

A handwritten signature in black ink, appearing to read 'Cambria Haydon', with a stylized, flowing script.

Cambria Haydon  
Chief Privacy Officer  
Providence St. Joseph Health

(Enclosure)



## Recommended Steps to Help Protect Your Information

**1. Website and Enrollment.** Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**4. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**5. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**6. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392.

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.