Grays Harbor COMMUNITY HOSPITAL

Caring for the Harbor

14 August 2019

Washington State
Office of the Attorney General
1125 Washington St. SE
Olympia, WA 98501

To Whom It May Concern,

In accordance with RCW 19.255.010(10) and (15), Grays Harbor Community Hospital (GHCH) and Harbor Medical Group (HMG) provide notification to the Washington State Attorney General of a breach of the security of GHCH's and HMG's electronic systems that have affected the personal information of over 500 Washington consumers. Attached to this e-mail is a sample copy of the security breach notification notice that GHCH and HMG sent to Washington consumers affected by the breach. As described in the letter, this breach was caused by a ransomware attack. At this time, GHCH and HMG estimate that approximately 88,000 Washington State consumers were affected by the breach.

Sincerely,

Jason G. Halstead
Director of Quality, Risk, and Compliance
Privacy Officer

GRAYS HARBOR COMMUNITY HOSPITAL

HARBOR MEDICAL GROUP

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>>

Ransomware Incident Notification

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

This letter is to inform you of a ransomware incident that recently occurred, impacting some of your health care information maintained by Grays Harbor Community Hospital ("GHCH") and Harbor Medical Group ("HMG").

On June 15, 2019, GHCH and HMG discovered that databases containing your electronic medical record were encrypted by a sophisticated software program designed to block access to a computer system until a sum of money is paid, otherwise known as ransomware. Upon identifying the ransomware, GHCH and HMG launched an immediate investigation with the support of leading forensics and network consultants, and the investigation is ongoing. GHCH and HMG also notified the FBI of the incident.

After taking the appropriate precautions to safeguard the network, GHCH and HMG used established backup procedures to recover much of your health care information; however, certain parts of your electronic medical record described below remain encrypted and inaccessible by GHCH and HMG. Please note that, at this time, GHCH and HMG have no reasonable basis to believe that any of your personal information has been transmitted outside of GHCH's or HMG's databases.

Your health information that was impacted by the ransomware may have included your full name, date of birth, social security number, phone number, home address, and medical record information, including dates of service, diagnosis, and treatment information. GHCH and HMG have utilized backup procedures to recover much of the information that was encrypted, but, as the date of this letter, GHCH and HMG have been unable to fully recover all of the health information affected by this incident.

GHCH and HMG will continue to work diligently with security experts to recover the affected databases and re-establish access to your entire electronic medical record. However, at this time, we cannot guarantee that we will be able to gain access to all of your electronic medical record files locked by the ransomware.

Ransomware incidents of this nature are different from other data incidents in that the data remains within the database. While GHCH and HMG do not believe that any of your personal information was transmitted outside of GHCH's or HMG's databases, out of an abundance of caution, GHCH and HMG are notifying you of the incident via this letter. GHCH and HMG have also arranged for you to enroll in a credit monitoring service through Experian. Please see the enclosed instructions on how to enroll in the credit monitoring service. This service is available to you at no cost.

We ask that you review the enclosed "Additional Resources" document included with this letter. The Additional Resources document describes steps that you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identity theft protection, and details on how to place a fraud alert or a security freeze on your credit file.

GHCH and HMG have and will continue to take steps to mitigate this incident and to help prevent this type of incident from happening again, including implementing more robust security and backup procedures to protect against ransomware attacks. We are also providing training for staff members to ensure that they understand how to avoid ransomware.

We sincerely apologize and regret that this situation has occurred. We take our responsibility to protect our patients' personal information very seriously. If you have further questions, please call 1-???-???-????, Monday through Friday, 7:30 a.m. to 5:00 p.m. Pacific Time.

Sincerely,

Tom Jensen
CEO

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<ClientDef1(Date)>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **<<Member ID>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057. Be prepared to provide the engagement number **<<ClientDef2(Engagement #)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 1-877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 1-877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Resources

Contact information for the three nationwide credit reporting agencies is:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes: (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

You may contact the **Washington State Attorney General**, Consumer Protection Division at 800 5th Ave, Suite 2000, Seattle, WA 98104-3188, https://www.atg.wa.gov/identity-theftprivacy.