January 29 , 2021

Sent via email: SecurityBreach@atg.wa.gov

Office of the Washington State Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Security Incident Notification

Dear Attorney General Ferguson:

This letter is to inform you of a recent data security incident involving one of Grays Harbor Community Hospital's ("GHCH") service providers. The affected service provider is Metro Presort, Inc. ("MPI"), who provides certain mail processing services to GHCH. This letter describes the incident, what MPI's investigation has revealed so far about the information involved and potentially affected individuals, and the measures MPI and GHCH have taken in response to the incident.

In a letter from MPI received by GHCH on November 29, 2020, MPI informed GHCH that on May 6, 2019, cybercriminals deployed ransomware throughout MPI's network and systems that locked MPI out of its systems and prevented it from accessing information used to process mailings. MPI explained that this incident was contained by May 15, 2019, when all affected systems were permanently disconnected, and the threat was neutralized using advanced software. MPI initially believed that customer data files containing patient information for mailings were already encrypted at the time of the attack and thus were not accessible. In October 2020, it reinvestigated this incident and determined that it could not be certain that these files were encrypted before the attack. Thus, according to MPI, there was a potential for unauthorized access of patient information, although there is no evidence of any improper access.

The U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"), investigated the incident, MPI's response, and MPI's data privacy and security practices. On December 31, 2020, OCR issued a letter in which it provided technical assistance to MPI and closed its investigation of the matter.

The customer files processed by MPI for GHCH which were potentially accessible as a result of the incident were for invoices and other statements. These documents included the following categories of information: names, addresses, and dates of birth, patient, health plan ID, or account numbers, treatment or appointment dates, and diagnosis or treatment codes, depending on what categories of information were included in mail files. This information includes "personal information" as that term is defined by RCW 42.56.590. Social Security numbers, financial account information, private keys, and username and passcodes for secure accounts were not included. MPI reports that there is no indication any personal information was actually improperly accessed, viewed, or used.

MPI reported that it has taken several steps to enhance its data security after the incident, including additional technical safeguards to prevent similar incidents in the future and additional protections (encryption) of customer files. According to MPI, it has notified law enforcement and is cooperating with their investigation. A web page created by MPI addressing the incident is available at https://www.metropresort.com/security-incident/.

Based on our investigation, we reasonably believe that approximately 5,136 GHCH patients are potentially affected by the incident, of which approximately 4,984 patients are Washington residents. In accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations, and in accordance with RCW 42.56.590, GHCH provided written notice of the data security incident to affected patients beginning on January 29, 2021. This notice provided guidance on how patients may protect themselves against identity theft and fraud. Sample notification letters are enclosed with this letter. On January 25, 2021, GHCH also issued a press release about the incident to prominent print media outlets serving the geographic areas where the individuals affected by the incident likely reside. On January 29, 2021, MPI provided notice to the Secretary of Health and Human Services on GHCH's behalf about the incident.

Although this security incident occurred with one of our service providers, GHCH has taken this opportunity to review our own security protocols and safeguards to protect the information maintained in our systems.

We will update the information in this letter as necessary under RCW 42.56.590.

Sincerely,

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

GRAYS HARBOR
COMMUNITY
HOSPITAL
915 Anderson Drive
Aberdeen, WA 98520

Label Numb

VIA FIRST-CLASS MAIL

January 26, 2021

Full Name1______________________________________50
Alternate 1 Address
Delivery Address
City St ZIP+4

NOTICE OF DATA SECURITY INCIDENT

Dear Salutation

We are writing to notify you that one of our service providers, Metro Presort, Inc. ("MPI"), experienced a data security incident – a ransomware attack – that may have involved your personal information. MPI is a printing and mail processing company that has processed notices, invoices, and other statements for us. According to information provided by MPI, there is no evidence that any patient information was improperly accessed or left its network or systems, but there was a potential for unauthorized access. We take our obligation to protect your privacy seriously and are thus sharing with you the information about this incident that we have received from MPI.

WHAT HAPPENED. According to MPI, on May 6, 2019, cybercriminals deployed ransomware throughout its network and systems that locked MPI out of its systems and prevented it from accessing information used to process mailings. MPI explained that this incident was contained by May 15, 2019, when all affected systems were permanently disconnected, and the threat was neutralized using advanced software. MPI initially believed that customer data files, including data files of Grays Harbor Community Hospital and Harbor Medical Group, containing patient information for mailings were already encrypted at the time of the attack and thus were not accessible. In October 2020, it reinvestigated this incident and determined that it could not be certain that these files were encrypted before the attack. Thus, according to MPI, there was a potential for unauthorized access of patient information, although there is no evidence of any improper access.

The U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"), which is the federal agency responsible for enforcing the federal health information privacy law known as HIPAA, investigated the incident, MPI's response, and MPI's data privacy and security practices. On December 31, 2020, OCR issued a letter in which it provided technical assistance to MPI and closed its investigation of the matter.

WHAT INFORMATION WAS INVOLVED. The customer files that MPI processed for us that were potentially accessible were for invoices and other statements. They included the following categories of information: names, addresses, and dates of birth, patient, health plan ID, or account numbers, treatment or appointment dates, and diagnosis or treatment codes, depending on what categories of information were included in mail files. Social Security numbers, financial account information, private keys, and username and passcodes for secure accounts were not included. Again, MPI reports that there is no indication any personal information was actually improperly accessed, viewed, or used.

<u>What MPI and We Are Doing</u>. MPI has reported that it has taken several steps to enhance its data security after the incident, including additional technical safeguards to prevent similar incidents in the future and additional protections (encryption) of customer files. According to MPI, it has notified law enforcement and is cooperating with their investigation. To learn more about the incident, you can visit a web page addressing the incident that MPI has created at https://www.metropresort.com/security-incident/. If we learn of any additional information that warrants further notice, we will notify you. Although this security incident occurred with one of our service providers, we have taken this opportunity to review our own security protocols and safeguards to protect the information maintained in our systems.

<u>What You Can Do To Protect Your Information</u>. Again, MPI has reported that there is no evidence of any improper access or use of your information, but you should always be vigilant when receiving and responding to correspondence or inquiries from unknown sources. You should regularly monitor your personal accounts and information for any unusual activity. If you notice any unusual activity, you should immediately notify your financial institutions (for example, your bank or credit card provider) and your healthcare providers.

In addition, please carefully review the enclosed summary of additional steps you can take to protect your personal information, which includes 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. It also includes the contact information for the three major credit reporting agencies and suggestions for obtaining and reviewing your credit report.

MPI has expressed its regret about this incident, and we likewise apologize to you. Again, please know that we take our responsibility to protect our patients' personal information very seriously. If you have any questions about this incident or concerns about the potential that your information was accessed, you may call the following toll-free number established by MPI: **833-971-3304** (8:00am to 5:00pm PST).

Sincerely,

Jason

Jason Halsead
Director of Quality, Risk and Compliance

Enclosure

IDENTITY THEFT PREVENTION AND PROTECTION

Monitor Your Accounts and Credit Reports, and Notify Police and the FTC of Suspicious Activity: When you receive account statements, credit reports, and monitoring alerts, review them carefully for unauthorized activity. Look for accounts you did not open, unauthorized purchases, inquiries from creditors that you did not initiate, and personal information that you do not recognize, such as a home address or Social Security number. If you have concerns, call your bank, the account provider, or the credit reporting agency. If possible, place a security verification secret word, similar to a password, on your accounts. If you suspect any fraudulent activity or identity theft, promptly report it to local law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to https://www.consumer.ftc.gov/features/feature-0014-identity-theft or call 1-877-ID-THEFT (877-438-4338). Request copies of any police or investigation reports created, as you might need to provide this information to credit reporting agencies or to supposed creditors to clear up your records.

Obtain Free Credit Reports**:** Even if you do not find any signs of fraud on your reports, you should check your credit report regularly. There are three main credit reporting agencies: Equifax, Experian, and TransUnion. Their contact information, along with contact information for the FTC and some state agencies, are on the reverse side. Each credit reporting agency must provide you annually with a free credit report, at your request made to a single, centralized source for the reports, AnnualCreditReport.com. You are not required to order all three reports at the same time; instead, you may rotate your requests so that you can review your credit report on a regular basis. In addition, many states have laws that require the credit reporting agencies to provide you with a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

Free Services by Credit Reporting Agencies**:** Each credit reporting agency offers additional free services to help you protect your credit. TransUnion at www.transunion.com permits you to sign up for TrueIdentity which is a service that allows you to examine your TransUnion credit file and place a “credit lock” which prevents others from opening up credit in your name. Experian at www.experian.com provides you with a free credit report every month when you select “Start with your free Experian Credit Report.” Equifax at www.equifax.com permits you to sign up for “Lock & Alert" which also allows you to place a credit lock.

Fraud Alert**:** You may ask the credit reporting agencies to place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three credit reporting agencies. As soon as that agency processes your fraud alert, it is supposed to notify the other two, which then also must place fraud alerts in your file. An *initial fraud alert* stays in your file for at least 90 days. An *extended alert* stays in your file for seven years. To place either of these alerts, a credit reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency.

Security Freeze: You also have the right to place a security freeze on your credit report at any of the three main credit reporting agencies. 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. If you choose to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail, the following information must be included when requesting a security freeze: (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.

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, and displays your name, current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the agency. The main three credit reporting agencies provide details about their security freeze services and state requirements at the following links:

- Experian: http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/
- Equifax: https://help.equifax.com/app/answers/detail/a_id/159 & https://help.equifax.com/app/answers/detail/a_id/75/~/security-freeze-fees-and-requirements
- TransUnion: https://www.transunion.com/credit-freeze/place-credit-freeze

Internal Revenue Service: Tax-related identity theft is when someone uses your Social Security number to file a false tax return claiming a fraudulent refund. If you received IRS correspondence indicating you may be a victim of tax-related identity theft or your e-file tax return was rejected as a duplicate, do the following:

- Submit an IRS Form 14039, Identity Theft Affidavit, to the IRS;
- Continue to file your tax return, even if you must do so by paper, and attach the Form 14039; and
- Watch for any follow-up correspondence from the IRS and respond quickly.

The fillable IRS Form 14039 is available at IRS.gov. Follow the instructions exactly. You can fax or mail it or submit it with your paper tax return if you have been prevented from filing because someone else has already filed a return using your SSN. You only need to file it once. Do not respond to threats made over the phone or via email that the IRS will take action against you. The IRS will communicate with you in writing.

Financial Accounts, Oral Passwords and 2FA: If financial accounts are affected, contact the institution and ask them about steps you may take to further protect your account. Financial institutions will often permit you to place an oral password on your account or enable multifactor authentication to your online account.

Contact Information for the FTC, Credit Reporting Agencies, and State Consumer Protection Agencies: If you suspect fraudulent activity on any of your financial accounts (savings, checking, credit card) or identity theft, you are encouraged to report your concerns to your financial institutions and the relevant agencies below.

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

AnnualCreditReport.com
Annual Credit Report Request
Service
P.O. Box 105281
Atlanta, GA 30348-5281
www.annualcreditreport.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com