



Wes Moore, Governor · Aruna Miller, Lt. Governor · Laura Herrera Scott, M.D., M.P.H., Secretary

December 16, 2024

Mr. Jeff Karberg
Maryland Office of the Attorney General
200 St. Paul Place, Baltimore, Maryland 21202
Baltimore, Maryland 21202

via email: jkarberg@oag.state.md.us

Re: Maryland Department of Health Notice pursuant to Maryland State Government Article § 10-1305(h)

Dear Mr. Karberg:

On September 27, 2024, the Office of Internal Controls, Audit Compliance & Information Security (IAC/S) was notified by the Garrett County Health Department's (GCHD) Health Officer of a potential Health Information Portability and Accountability Act and Protection of Information by Government Agencies Act violation. The breach occurred on or about September 24, 2024.

GCHD uses an electronic health record system, PatTrac. This system has a public facing web site that allows citizens to search the permits and inspection reports of food service facilities located in Garrett County. A task notification was inadvertently linked to the web site which, when clicked, allowed individuals to access confidential patient information. This occurred due to the employees that were assigned the task not having user names attached to their employee name. This incident may have resulted in disclosure of the following types of protected health information: patient name, address, sex, age, date of birth, the type of clinic that the patient visited, insurance information, and an image of their driver's license. Two clients were affected by this breach.

Sincerely,

Kathryn Hoffman
Health Policy Analyst
Office of Internal Controls, Audit Compliance & Information Security
Maryland Department of Health
201 West Preston Street - 5th Floor
Baltimore, Maryland 21201

October 23, 2024

Michael A. Gibson
5794 Goode Road
Hughesville, MD 20637
michael@michaelgibson.com
(301) 638-4480

Dear [REDACTED],

We regret to inform you of an incident involving your protected health information. On September 24, 2024, we discovered a security breach. As a result, some of your protected health information may have been accessed, used, or disclosed.

What Happened? The Garrett County Health Department uses an electronic health record system, PatTrac, to store patients' medical history and treatment plans to improve patient care and efficiency, as well as to reduce costs. This system has a public-facing website that allows citizens to search for permits and inspection reports of food service facilities located in Garrett County. A task notification was inadvertently linked to the website, which, when clicked, allowed individuals to access confidential patient information.

What information was involved? This incident may have resulted in disclosure of the following types of your protected health information; Your Name, Address, Sex, Age, Date of Birth, the type of clinic that you visited, Insurance information, and an image of your Driver's License.

What we are doing? We have taken appropriate steps to mitigate the security incident and to prevent similar incidents from happening in the future.

What you can do: We have no reason to believe that you are at an increased risk of identity theft as a result of the security incident. However, we encourage you to take the following additional steps:

- Call a credit bureau of your choosing to place a fraud alert on your credit report, which can assist in the prevention of identity theft. Once one credit bureau has received your request, they will notify the others for your protection. Three credit bureaus listed on <https://www.usa.gov/credit-reports> are included below for your convenience. Please review the website for further credit report information.

Equifax:

800-685-1111

<https://www.equifax.com/personal/credit-report-services/>

Equifax Information Services LLC, PO Box 105788, Atlanta, GA 30348-5788

TransUnion:

888-909-8872

<https://www.transunion.com/credit-freeze>

TransUnion LLC, PO Box 2000, Chester, PA 19016

Innovis:

800-540-2505

<https://www.innovis.com/securityFreeze/index>

Innovis Customer Assistance, PO Box 26, Pittsburgh, PA 15230-0026

- Review your credit reports. When you receive your credit reports, examine them closely to look for signs of fraud, such as credit accounts that are not yours. You may also establish a fraud alert. By establishing a fraud alert, you will receive a follow-up letter that explains how to receive a free copy of your credit report.
- Continue to monitor your credit reports. Even when a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure account(s) were not falsely opened with your personal information.
- If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. 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 law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

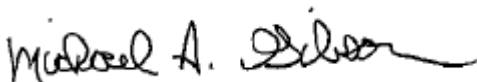
Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Maryland Attorney General's Office
Identity Theft Unit
200 St. Paul Place, 25th Floor
Baltimore, Maryland 21202
www.marylandattorneygeneral.gov
idtheft@oag.state.md.us
1-410-576-6491
1-888-743-0023

We sincerely regret that this security incident occurred. Please do not hesitate to contact us with questions about this incident or additional information as a result of the incident.

Michael A. Gibson
301-638-4480
michael@michaelgibson.com
5794 Goode Road
Hughesville, MD 20637

Sincerely,



Michael A. Gibson
Software Developer