NOTICE OF DATA PRIVACY INCIDENT

The Georgia Department of Public Health ("DPH") is providing notice of an event which may impact the privacy of information related to certain individuals. While DPH is unaware of any attempted or actual misuse of the information at this time, DPH will be notifying potentially affected individuals, and in those notifications, will provide information about the event, steps taken since learning of the event, and on what a potentially impacted individual can do to better protect against potential misuse of their personal information, should they feel it appropriate to do so.

What Happened? The Georgia Technology Authority ("GTA") notified the Georgia Department of Public Health ("DPH") that its email services provider, contracted through GTA, became aware of unauthorized access to the email accounts of certain DPH employees that contained information DPH considered to be confidential. Upon becoming aware of this information, GTA and other state partners immediately took steps to secure the email accounts and launched an investigation to determine the nature and scope of the activity. Although DPH and GTA have no evidence to indicate that any information related to individuals was actually viewed, they are providing notice out of an abundance of caution.

Upon becoming aware of the unauthorized access, GTA began a diligent and comprehensive review process to identify sensitive information that may have been contained within the impacted email accounts, and to identify the individuals whose information may have been impacted. That process recently completed, and DPH is attempting to locate current address information for potentially impacted individuals and is also assessing with what entities those individuals may be affiliated. DPH will be providing written notification to potentially impacted individuals for whom they can locate an address once their review completes.

What Information Was Involved? While the actual types of data impacted vary by individual, the investigation determined that the following types of information may be impacted: names, Social Security numbers, financial account information, driver's license information, dates of birth, and medical information, including but not limited to, medical record numbers, diagnosis information, treatment information, and physician information. At this time, DPH has no evidence that individuals' information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among DPH's and GTA's highest priorities. Upon learning of the incident, DPH, GTA, and other partners took immediate steps to secure our email environment.

For More Information. If you have additional questions, please contact DPH's toll-free dedicated assistance line at 1-833-833-3755, Monday through Friday, excluding holidays, from 8:00 am to 8:00 pm Eastern time. You may also write to DPH at 200 Piedmont Avenue, SE, Atlanta, GA 30334.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. Additionally, we encourage individuals to check their medical records to ensure that there have not been any unexpected changes. Individuals have the right to ask their medical providers to place restrictions on their medical records to safeguard their data. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit https://www.annualcreditreport.com or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three (3) major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help/

1 (888) 298-0045	1 (888) 397-3742	1 (800) 916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; https://www.identitytheft.gov; 1 (877) ID-THEFT (1 (877) 438-4338); and TTY: 1 (866) 653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, the Federal Trade Commission, and the relevant state Attorney General. This notice has not been delayed by law enforcement.