The Commonwealth of Massachusetts
Executive Office of Health & Human Services
Department of Developmental Services
40 Broad Street, 4th Floor
Boston, MA 02109

MAURA T. HEALEY
GOVERNOR

KIMBERLEY DRISCOLL
LIEUTENANT GOVERNOR

KIAME J. MAHANIAH
SECRETARY

SARAH W. PETERSON
COMMISSIONER

Phone: (617) 727-5608
Video Phone: (857) 366-4179
www.mass.gov/dds

March 19, 2026

[redacted]

Dear [redacted]:

I am the Massachusetts Department of Developmental Services ("DDS" or the "Department") Privacy Officer, and I am writing to follow up with you about your report of receiving unencrypted email containing "protected health information", as defined in the Health Insurance Portability and Accountability Act ("HIPAA", 45 CFR Part 164), and "personal information", as defined in G.L. c. 93H, § 1, from DDS.

What happened?

On February 19, 2026, I received an email from you stating, "I want to inform you of the following event that occurred on January 20, 2026, for your consideration of appropriate next steps. On this date, copies of [redacted] where sent unencrypted to external e-mail addresses by Department of Developmental Services (DDS) employees. This was in response to an e-mail where I had requested a secure method to transmit this information for [redacted]. I am concerned about the breach of Personal Identifiable Information (PII) and Protected Health Information (PHI) that occurred in this instance and the long term impact it may have on my [redacted]. Please let me know if there is any additional information you need and what further steps need to be taken." DDS Ombudsperson Meghan Allen was also listed as a recipient of your February 19th email.

You and I spoke via telephone on February 20th. You reported to me that the unencrypted transmission occurred when you were communicating with a DDS employee via unencrypted email. This employee then cc'd another DDS employee, [redacted]

[redacted]. You told me that you requested a secure email link to transmit [redacted] materials to DDS, but before the secure link was provided to you, [redacted] "replied all" to the email and attached the [redacted] The "reply all" email was addressed to the other involved DDS employee (via mass.gov) and to you and your spouse's personal email addresses (external non-mass.gov email addresses).You told me that one of the DDS employees involved immediately sent you a secure link and apologized for the unencrypted transmission.

You indicated to me that you believed this to be inadvertent on DDS' part, but that you also considered this to be a serious breach. You requested credit monitoring services, and I informed you that the Commonwealth's position is that the credit monitoring services requirements of G.L. c. 93H do not apply to Commonwealth agencies. I informed you that I would conduct a risk assessment and follow up with you in writing. I also suggested that you and your wife remove or delete the information from your email mailboxes if you had not already done so.

What information was involved?

The [redacted] attached materials contained full name, address, health insurance information, bank account number and full nine-digit social security number. Additionally, there was PHI contained [redacted]. G.L. c. 93H defines "Personal information" defines as: "a resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

(a) Social Security number;
(b) Driver's license number or state-issued identification card number; or
(c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account."

What is DDS doing?

When I learned of this incident, I immediately requested and confirmed that the involved DDS employees removed the attachment from their Outlook mailboxes. DDS will take other personnel action it may deem necessary. Please note that DDS has mandatory yearly HIPAA and security training requirements, and supervisors have assigned additional training as warranted. As a result of the type of information involved and your request that PII be sent with encryption, DDS is implementing the reporting pursuant to G.L. c. 93H.

DDS is not aware of any suspicious activity and has no information or reason to believe that this information was sent to or accessed by unintended or unauthorized recipients, or that it was intercepted during transit or in rest. I sincerely appreciate that you reported receiving unencrypted PHI/PII from DDS and I wanted to follow up with you to let you know that DDS has investigated this incident. DDS will assess its year-end reporting obligations in relation to this incident and will

include this incident in its year-end reporting as applicable. I also wanted to inform you about steps you can take to protect personal and protected health information going forward.

What can you do?

DDS encourages you to remain vigilant against incidents of identity theft by reviewing financial account statements for unusual activity and reporting any suspicious activity immediately to their financial institution. You may wish to consider taking additional precautionary measures to protect against identity theft or other fraud including, but not limited to, the placement of fraud alerts on your child's credit file; review of credit reports for any unexplained activity; and review of credit card or other financial statements or accounts for any suspicious or unauthorized activity. You can also visit https://www.usa.gov/credit-reports to learn about obtaining a free annual credit report.

Under Massachusetts law, you have the right to obtain any police report filed regarding this incident. If there has been an instance of identity theft, you have the right to file a police report and obtain a copy of it. I have included the required notifications below should you have concerns regarding identity theft or other inappropriate use of her identity or credit.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware that requesting a security freeze may delay, interfere with, or prevent the timely approval of any requests made for new loans, credit, mortgages, employment, housing or other services. If an individual is a victim of identity theft and provides the credit reporting agency with a valid police report, it cannot charge to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on a credit report, you must send a written request to each of the three (3) major consumer reporting agencies: Equifax; Experian; and TransUnion by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O Box 105788 Dept. Atlanta, GA 30348 1-888-298-0045	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-EXPERIAN (397-3742)	Trans Union Security Freeze Fraud Victim Assistance P.O. Box 6790 Fullerton, CA 92834 1-800-680-7289

You may also submit a credit freeze online at the following websites:

Equifax Security Freeze: https://www.equifax.com/personal/help/article-list/-/h/a/place-lift-remove-security-freeze

Experian Security Freeze: https://www.experian.com/help/credit-freeze/

Trans Union Security Freeze: https://www.transunion.com/credit-

freeze?atvy=%7B%22261809%22%3A%22Experience+B%22%7D

In order to request a security freeze for an individual, you will need to provide the following information for them:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. Address, and all residential addresses lived at in the last 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 I D card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, Investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on the credit report. The credit bureaus must also send written confirmation within five (5) business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal of the security freeze. To remove the security freeze to allow a specific entity or individual access to the credit report, a written request to the credit reporting agencies must be sent by mail and must include proper identification (name, address, and social security number) and the PIN number or password provided when the security freeze was placed as well as the identities of those entities or individuals you would like to receive the credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified time period.

To remove the security freeze, you must send a written request to each of the three (3) credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided when the security freeze was placed. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Please be assured that the Department takes its duty to protect PHI/PII extremely seriously, and I would note that your reporting of this incident not only helps to protect other DDS service recipients but also reinforces best practices for DDS staff. We apologize for any inconvenience or concern you've experienced.

If you have any questions or additional concerns, please feel free to contact the DDS Privacy Office at dds.privacy.officer@mass.gov.

Sincerely,

/s/ Erin G. Brown

Erin G. Brown
Deputy General Counsel, Privacy and Records
DDS Privacy Officer