The Commonwealth of Massachusetts
Executive Office of Health & Human Services
Department of Developmental Services
1000 Washington Street
Boston, MA 02118

MAURA T. HEALEY
GOVERNOR

KIMBERLEY DRISCOLL
LIEUTENANT GOVERNOR

KATHLEEN E. WALSH
SECRETARY

SARAH W. PETERSON
ACTING COMMISSIONER

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

November 7, 2024

By First Class Mail

[redacted]

Re: Notice of Unauthorized Disclosure of Protected Health Information

Dear: [redacted]

I am the Massachusetts Department of Developmental Services ("DDS" or the "Department") Privacy Officer, and I am writing to notify you that an unauthorized disclosure of "protected health information" ("PHI"), as defined in the Health Insurance Portability and Accountability Act ("HIPAA", 45 CFR Part 164), belonging to [redacted] and maintained by DDS occurred.

What happened?

On July 30, 2024, DDS was notified by the Massachusetts Executive Office of Technology Services and Security ("EOTSS"), the Commonwealth agency responsible for supervising the information technology ("IT") services of all agencies within the executive department, of an e-mail phishing attack targeted at Commonwealth of Massachusetts employees and that a small number of DDS employee email accounts were considered compromised as a result.[13] On September 30, 2024, DDS notified the individuals affected by this event. In the course of DDS' continued investigation, on September 10, 2024, EOTSS and DDS discovered that additional information was compromised by the phishing attack.

[13] Phishing is one of the most common tactics used in online identity theft and cybercrimes. Using elements of social engineering, phishing is the fraudulent attempt to obtain a user's sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Using elements of social engineering, phishing is the fraudulent attempt to obtain a user's sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. https://www.mass.gov/info-details/smstext-message-phishing

What information was involved?

The information that was compromised includes contact information (such as name, address, date of birth, phone number, email) and one or more of the following:

- Health information (healthcare providers, diagnoses, medicines, and care and treatment information)
- Personal information (Social Security number, driver's license or state ID number, or other ID number)

This incident also constitutes a "breach of security" as pursuant to G.L. c. 93H, § 1, which defines "breach of security" as: "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth." *See* G.L. c. 93H, § 1. "Personal information" is defined as: "a resident's first name and last name or first initial and last name in combination with any 1 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; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." *See* G.L. c. 93H, § 1.

What is DDS doing?

In accordance with state and federal privacy and confidentiality laws, DDS is notifying you of the unauthorized disclosure of your protected health information and personal information. DDS will implement corrective measures to protect against further unauthorized disclosures or acquisitions, and all appropriate supervisory and personnel measures will be taken. All DDS email accounts have since been secured and no further IT security remediation is outstanding.

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 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. Please contact me if you would like information on how to do this.

Please be assured that the Department takes its obligation to protect the personal and protected health information of the individuals we support very seriously. We apologize for any inconvenience or concern you've experienced.

If you should have any further questions, please call DDS toll-free at 1-833-486-7686. You can also email us at dds.privacy.officer@mass.gov.

Sincerely,

/s/ Erin G. Brown

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