

SAMPLE NOTIFICATION OF BREACH TO STATE AND FEDERAL OFFICIALS

[Date]

*Notice to the Secretary of Health & Human Services may be provided using the HHS/OCR website:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

Secretary of Health & Human Services
The U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

*In the event the unsecured PHI includes “personal information” of Massachusetts residents [“personal information” means a Massachusetts 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], regardless of the number of affected individuals, then notice must also be sent to:

Attorney General Maura Healey
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Director of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116

Dear Secretary/Attorney General Healey/Director:

In compliance with Massachusetts data security law and the Health Insurance Portability and Accountability Act (“HIPAA”), I am notifying you of a recent breach of unsecured protected health information (“PHI”) [and personal information] of Massachusetts residents. I discovered the breach on [Date and Time]. The breach involved [number] of patients. The following occurred:

Describe what happened in general terms, including:

- *A brief description of what happened, including the date the breach actually occurred, if known*
- *Where the breach occurred*
- *Who used the PHI [and personal information] or to whom the disclosure of PHI and personal information was made, including whether it was a Covered Entity or Business Associate*
- *What kind of PHI [and personal information] was involved in the breach (e.g., full name, social security number, date of birth, home address, patient ID number or billing number, diagnosis, insurance information, etc.)*
- *Whether the PHI [and personal information] was actually viewed or accessed*
- *Mitigation efforts*

I also relayed the following information to my patients(s): See attached form letter sent to patients.

Optional:

I have also established a section on my web site with updated information on this breach. You can reach my web site at: [insert web site address].

If you have any questions or require further information, please contact me at [insert contact information].

Sincerely,

[Insert Name]

1703496v1/14993-3