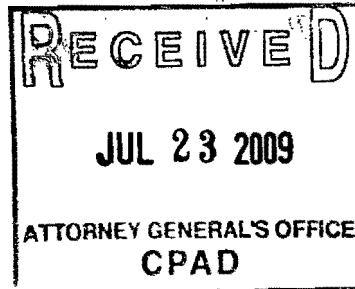


Rebecca L. Rausch  
rrausch@kb-law.com

July 22, 2009

**VIA CERTIFIED MAIL,**  
**RETURN RECEIPT REQUESTED**



Scott Schafer, Chief  
Consumer Protection Division  
Office of the Attorney General  
One Ashburton Place  
Boston, MA 02108

David Murray, Esq.  
Office of Consumer Affairs and Business Regulation  
Ten Park Plaza, Suite 5170  
Boston, MA 02116

**Re: Notification of Security Breach pursuant to Chapter 93H**

Dear Messrs. Schafer and Murray:

This office represent The May Institute, Inc. ("The May"). This letter is designed to comply with the notification requirements set forth in Section 3(b) of Chapter 93H of the Massachusetts General Laws.

The May is a nationally recognized provider of educational, behavioral health, and rehabilitative services. As a regular part of its business, The May enters into contracts with various state agencies to provide services falling under such agencies' jurisdictions. Recently, The May engaged in its annual contract renewal process with both the Department of Mental Retardation ("DMR") and the Department of Mental Health ("DMH"). Part of the DMR contract renewal required The May to submit a list of individuals served in the Mashpee service area, which list included, among other things, the full names and social security numbers of those individuals. The list contained personal information about sixty-four (64) Massachusetts residents.

On May 21, 2009, The May inadvertently enclosed a single hard copy of the list in the contract renewal packet it sent to DMH, instead of the contract renewal packet for DMR. The recipient at DMH notified The May of the disclosure on May 26, 2009. The May instructed DMH to either return or destroy the sole copy of the list and, in response to that request, DMH shredded and destroyed its only copy of the list. The May received confirmation that the disclosed copy of the list had been destroyed on May 28, 2009.



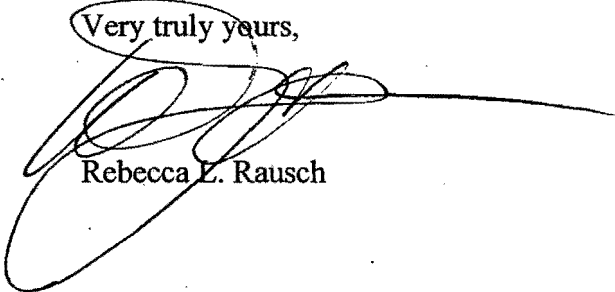
Scott Schafer  
David Murray  
July 22, 2009  
Page 2

Subsequent to this incident, The May has discussed the importance of ensuring that information is sent to the correct recipient with the employee who inadvertently sent the list to DMH instead of DMR, and generally reminded all of its employees to double-check all packages containing personal information for accuracy before sending any such packages. Also, on July 13, 2009, The May issued the resident notification required by Chapter 93H, a copy of which is enclosed. Please note that the resident notification was designed to comply with both Chapter 93H and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as recently amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act"), as The May is a covered entity under HIPAA. Section 13402(f) of the HITECH Act requires that the notification include "[a] brief description of what happened" and "[a] description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code)."

Given that the breach involved only one hard copy of the list and that hard copy was shredded and destroyed with no subsequent disclosures, The May believes the resulting risk of identity theft or fraud against the affected residents is minimal, if any.

Please contact me if The May should take any further action with regard to this incident.

Very truly yours,



Rebecca L. Rausch

Enclosure

cc: Terese Brennan, The May Institute, Inc. (via email only)

0362\0100\250688.2

July \_\_, 2009

**VIA CERTIFIED MAIL,**  
**RETURN RECEIPT REQUESTED**

<guardian name>  
<guardian address>

**Re: Personal Information of <first name> <last name>**

Dear <guardian name>:

This notification letter is provided to you in your capacity as guardian of <first name> <last name> and is designed to comply with Chapter 93H of the Massachusetts General Laws and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as recently amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").

As you know, <individual served> resides at our group home facility located at <individuals address>. On May 26, 2009, it came to our attention that his/her personal information (full name and social security number) was inadvertently sent to the wrong state funding agency. Specifically, the personal information was sent to the contract office of the Department of Mental Health (DMH) instead of the Department of Mental Retardation.

Please be assured that May Institute has taken appropriate steps toward remedying the situation. At May Institute's request, DMH shredded and destroyed the only copy of the personal information that it received. In addition, we have reminded employees that they should double-check packages containing personal information for accuracy before sending out those packages. Because only one copy of the personal information was released and we have received confirmation that they copy was destroyed, we believe that the risk of identity theft or other fraud is minimal.

Nonetheless, under state law, we are obligated to notify you of your option to place a security freeze on <individual served>'s accounts to protect his/her identity and credit rating. A security freeze is a notice placed on a credit report by a consumer reporting agency at your request. The security freeze prohibits the consumer reporting agency from releasing the credit report or any information in it without your express authorization. Since most businesses will not open credit accounts without first checking a consumer's credit history, a security freeze may help to prevent credit, loans, or other services from being approved in <individual served>'s name without your explicit consent.

To request a security freeze, send a written request to each of the three consumer reporting agencies. (The agencies will not share your request with each other.) The

written request must include all of the following information about <individual served>: (1) full name; (2) social security number; (3) date of birth; (4) current address; and (5) previous addresses for the past two years. In addition, you must include a copy of a government-issued identification card for <individual served>, such as a driver's license or a state or military ID card, and a copy of a utility bill, bank, or insurance statement. The security freeze should take effect within three (3) business days after receiving your request and will remain in place for seven (7) years unless you choose to lift it earlier. To lift the security freeze, again contact the three consumer reporting agencies. Each agency may charge a fee of up to five dollars (\$5.00) for placing, lifting, or removing a freeze.

Additional information about security freezes may be obtained from the Massachusetts Office of Consumer Affairs and Business Regulation by calling its consumer hotline at 617-973-8787 or 888-283-2757 (toll free within Massachusetts) or visiting its website. You can also contact the consumer reporting agencies directly:

- Experian (888-397-3742 or [www.experian.com](http://www.experian.com));
- Equifax (888-766-0008 or [www.equifax.com](http://www.equifax.com)); and
- TransUnion (888-909-8872 or [www.transunion.com](http://www.transunion.com)).

---

Please note that no police report has been filed in this case because the sole copy of the released personal information was destroyed and no theft or other criminal act occurred.

As always, we are available to offer support and address any questions or concerns you might have. If you have any further questions, please feel free to contact me at 781-440-0400 ext. 225.

Sincerely,

Terese Brennan  
Quality Improvement Department

0362\0100\249912.2

