Muscular Dystrophy Association, Inc.

Health Privacy and Security Policy -- Volunteers

Introduction & Purpose of Policy:

Muscular Dystrophy Association, Inc. ("MDA") is committed to protecting the privacy of the individuals and families that it serves, which includes ensuring the proper protection and treatment of Protected Health Information (PHI) and Electronic PHI (ePHI) (as such terms are defined in Appendix A). In addition, MDA is bound by the terms of certain federal and state health privacy laws, which were designed to ensure the privacy and security of PHI and ePHI.

The purpose of this Health Privacy and Security Policy (this "Policy") is to provide information to MDA volunteers with respect to the proper treatment of PHI. If you should have any questions about this Policy please contact your MDA district's executive director or MDA's Health Care Service Department, healthcareservices@mdausa.org.

Privacy and Security Principles:

In order to ensure the privacy and security of PHI and ePHI, MDA must (i) protect all PHI from inappropriate access, use or disclosure, and (ii) ensure the confidentiality, integrity and availability of ePHI. In order for MDA to comply with these privacy and security principles, the following apply to PHI:

- You may only access or use PHI if it is relevant to your volunteer function and if you are authorized by current MDA staff to access or use such information. Such access or use of PHI must be limited to the minimum amount of PHI necessary to perform your volunteer function.
- You may only disclose PHI to other MDA staff members or volunteers (who have a need-to-know) for the purpose of MDA's business operations. Such disclosure of PHI must be limited to the minimum amount of PHI necessary to accomplish the intended purpose of the disclosure.
- You may not access, use or disclose PHI for any other reason, including for fundraising purposes, to any person (whether MDA staff/volunteers or non-MDA staff/volunteers) without first confirming with MDA that the Association has secured written authorization from the individual (or his/her parent or legal guardian, where applicable) specifically allowing for such access, use or disclosure.
- You must take reasonable steps to safeguard and protect all PHI and ePHI that is in your possession or control.

Reasonable Steps in Safeguarding and Protecting PHI:

You should take the following steps to ensure the proper protection and safeguarding of PHI and ePHI:

- When working in an open setting, speak in an appropriate tone of voice. Do not discuss PHI where others can hear you.
- Do not leave documents containing PHI out in plain view (such as on your desk).
- Keep file cabinets, doors and desks that contain PHI locked when not attended.
- Do not leave documents containing PHI unattended on the photocopier, printer or fax machine. When you are finished photocopying, printing or faxing documents containing PHI, check all areas of

the photocopier, printer and/or fax machine to ensure you have collected and removed all of the documents.

- Shred all documents containing PHI before disposing of them.
- Take care to properly secure PHI on your computer and to ensure that others cannot view or access such information. When you are away from your computer, log off of your computer or use a password-protected screensaver.
- Do not share your password(s) with anyone. Treat your password(s) as you would treat any piece of personal and confidential information by taking reasonable measures to keep it confidential. Do not post written password(s) in plain view or in an area easily accessible to others.
- Do not include PHI or ePHI in email communications
- If you are faxing a communication that contains PHI, confirm the fax number and email addresses of the intended recipients.
- Do not store PHI on mobile storage devices (such as flash drives, external hard drives, etc.),
- Do not leave brief cases (or other files or folders) that contain print PHI or laptops or other mobile electronic devices that contain ePHI unattended in a public place or in an unlocked vehicle (and, if unavoidable, lock the briefcase or device out of sight in the trunk and lock the vehicle).
- Dispose of electronic media that contains PHI properly. Contact your MDA district executive director for instructions about proper disposal.

Reporting Suspected Problems and/or Breaches:

If you feel that the privacy or security of PHI or ePHI may have been violated, report the incident immediately to MDA's privacy officer in the Health Care Service Department, healthcareservices@mdausa.org. MDA prohibits retaliation against anyone for raising, in good faith, a concern or question about the possibility of a breach of privacy.

Sanctions:

If you violate this Policy, MDA may need to withdraw your volunteer privileges. In addition, those who violate applicable state and federal health privacy laws may face civil and criminal penalties.

Policy Date: December 2014

VOLUNTEER ACKNOWLEDGMENT AND AGREEMENT:

I acknowledge that I have read and understand MDA's Health Privacy and Security Policy and agree to comply with its terms. I also acknowledge that I have completed MDA's online HIPAA training for volunteers and that I should contact staff at my nearest MDA office if I have any questions.

Signature: _____ Print Name: _____

Date: _____

APPENDIX A

DEFINITIONS

Protected Health Information (PHI):

- Protected Health Information (PHI) is any health information that may reveal the identity of a person and relates to: (1) past, present or future physical or mental health condition; or (2) healthcare services provided; or (3) payment for healthcare. PHI includes all communication media – whether written, electronic or verbal.
- Identifiers of PHI include:
    - Name
    - Street Address, City, County, Precinct, Zip Code
    - Dates (except year) that directly relate to a person (including birth date, admission date, discharge date, date of death, and all ages over 90)
    - Telephone numbers
    - Fax number
    - E-mail addresses
    - Social Security numbers
    - Medical record number
    - Health plan beneficiary number
    - Account number
    - Certificate/license number
    - Vehicle identifiers and serial numbers, including license plate numbers
    - Device identifiers and serial numbers
    - Web Universal Resource Locator (URL)
    - Internet Protocol (IP) address number
    - Biometric identifiers (for example, finger prints or voice prints)
    - Full-face photographs or similar images
    - Any other unique identifying number, characteristic or code

Electronic Protected Health Information (ePHI):

- Electronic PHI (or ePHI) means any PHI that is maintained or transmitted by electronic media.
- Some examples of ePHI may include:
    - PHI stored on memory devices on hard drives and any removable/transportable digital memory medium (such as on disk or digital memory device).
    - PHI transmitted via the Internet or Intranet (such as e-mails) or via physical movement of removable/transportable electronic storage media.