



1201 L Street, NW, Washington, DC 20005-4046
Main Telephone: 202-842-4444
Main Fax: 202-842-3860 2nd Main Fax: 202-842-3924
Writer's Telephone:
Writer's E-Mail:
www.ahca.org

Rick Miller
CHAIR
Avamere Health Services Inc.
Wilsonville, OR

Robert Van Dyk
VICE CHAIR
Van Dyk Health Care
Ridgewood, NJ

Angelo S. Rotella
IMMEDIATE PAST CHAIR
Friendly Home
Woonsocket, RI

Gail Clarkson
SECRETARY/TREASURER
The Medilodge Group Inc.
Bloomfield, MI

Neil Pruitt, Jr.
EXECUTIVE COMMITTEE LIAISON
UHS-Pruitt Corporation
Norcross, GA

Lane Bowen
AT-LARGE MEMBER
Kindred Healthcare
Louisville, KY

Richard Kase
AT-LARGE MEMBER
Cypress Health Care Management
Sarasota, FL

William Levering
AT-LARGE MEMBER
Levering Management Inc.
Mt Vernon, OH

Rick Mendlen
AT-LARGE MEMBER
Kennon S. Shea & Associates
El Cajon, CA

Richard Pell, Jr.
AT-LARGE MEMBER
Genesis HealthCare Corporation
Kennett Square, PA

Leonard Russ
AT-LARGE MEMBER
Bayberry Care Center
New Rochelle, NY

Van Moore
DD RESIDENTIAL SERVICES MEMBER
Westcare Management
Salem, OR

Wade Peterson
NOT FOR PROFIT MEMBER
MedCenter One Care Center
Mandan, ND

Howie Groff
NCAL MEMBER
Tealwood Care Centers
Bloomington, MN

James Carlson
ASHCAE MEMBER
Oregon Health Care Association
Portland, OR

Gail Rader
ASSOCIATE BUSINESS MEMBER
Care Perspectives
Phillipsburg, NJ

Bruce Yarwood
PRESIDENT & CEO

May 21, 2009

The Honorable Kathleen Sebelius
Secretary
Office of the Secretary of Health and Human Services
U.S. Department of Health and Human Services
200 Independence Ave. S.W.
Washington, D.C. 20201

Re: 45 CFR Parts 160 and 164
Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information, 74 Federal Register 19006, (April 27, 2009)

Dear Secretary Sebelius:

The American Health Care Association (AHCA), the National Center for Assisted Living (NCAL) and the Long Term Care Consortium (LTCC) appreciate the opportunity to comment on the above-referenced guidance. AHCA/NCAL is a federation of affiliated long-term care provider associations representing some 10,000 nonprofit and for-profit nursing facilities, skilled nursing facilities, assisted living and residential care facilities, sub-acute providers and intermediate care facilities for the mentally retarded and developmentally disabled. The LTCC is a group of AHCA/NCAL members with specific expertise in privacy, security and compliance—organized over eight years ago to provide leadership and guidance to the long term care profession and reduce the overall burden of compliance through collaboration on key initiatives.

AHCA/NCAL and its membership are committed to continuous improvement in the delivery of professional and compassionate care provided daily by millions of caring employees to more than 1.5 million of our nation's frail, elderly and disabled citizens who live in nursing facilities, assisted living residences and other facilities. The vast majority of our member long-term care facilities are covered entities under the Health Insurance Portability and Accountability Act (HIPAA). With the recent passage of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), HIPAA covered entities must now abide by enhanced patient privacy and security obligations including a heightened notification process.

Thus, AHCA/NCAL/LTCC have a direct interest in the *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Readable or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements*; and we subsequently offer our comments on the following questions specifically outlined in the new guidance:

1. Are there particular electronic media configurations that may render PHI unusable, unreadable, or indecipherable to unauthorized individuals, such as a fingerprint protected Universal Serial Bus (USB) drive, which are not sufficiently covered by the above and to which guidance should be specifically addressed?

We do not have additional suggestions for electronic media configurations that may render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

2. With respect to paper PHI, are there additional methods the Department should consider for rendering the information unusable, unreadable, or indecipherable to unauthorized individuals?

With respect to paper PHI, the current practice in LTC is to either contract with a shredding company or shred documents locally. This is the most convenient and acceptable method for destroying paper PHI in the LTC environment.

3. Are there other methods generally the Department should consider for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals?

We agree that encryption and de-identification of data will render electronic PHI unusable, unreadable, or indecipherable to unauthorized individuals. If PHI is on material that is not paper and cannot be shredded (e.g., pharmacy blister pack or IV packaging), we suggest that the Department allow providers to redact the PHI with a permanent marker, for example, prior to disposal.

4. Are there circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals?

We consider encryption, de-identification, shredding and redaction to all be reasonable methods for rendering PHI information unusable, unreadable, or indecipherable to unauthorized individuals.

5. Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals? Can risk of re-identification be alleviated such that the creation of a limited data set could be added to this guidance?

We believe that in most instances the risk of re-identification of a limited data set is very low and should be included in the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

6. In the event of a breach of PHI in limited data set form, are there any administrative or legal concerns about the ability to comply with the breach notification requirements?

Under most state breach laws, the disclosure of a limited data set does not meet the definition of a security breach. This is likely because identifying the harmed party in this situation is virtually impossible; and creates an insurmountable administrative burden for the provider to have to identify and notify the harmed individual.

7. Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?

We are concerned that naming off-the-shelf products is too limiting. Instead, we ask the Federal government to list the minimum requirements or standards that meet the applicable technological requirements.

The U.S. Department of Health and Human Services also asks the following general questions and we offer our comments as follows:

1. Based on experience in complying with state breach notification laws, are there any potential areas of conflict or other issues the Department should consider in promulgating the federal breach notification requirements?

The absence of express federal preemption of state health information privacy and security standards will pose real barriers to nationwide electronic health record adoption. Without a national set of patient privacy and security laws, we will find ourselves with multiple notifications, duplicate reporting requirements and fines. Anything short of federal preemption of state privacy and security laws will subject providers to inconsistent laws.

2. Given current obligations under state breach notification laws, do covered entities or business associates anticipate having to send multiple notices to an individual upon discovery of a single breach? Are there circumstances in which the required federal notice would not also satisfy any notice obligations?

Covered entities or business associates may have to send out multiple notices in instances of a single breach because each state statutory scheme has its own definition of a “breach” and a different process for how individuals must be notified. Neither the current Federal nor State laws satisfy the obligations under the others statutory scheme. Providers could draft notification that complied with both the Federal and State law, but this would have to be done for all 50 states, and would result in an excessive administrative burden for the provider and their business associates.

3. Considering the methodologies discussed in the guidance, are there any circumstances in which a covered entity or business associate would still be required to notify individuals under state laws of a breach of information that has been rendered secured based on federal requirements?

State laws have different definitions of “unsecured information” than found under the Federal laws. In many instances; therefore, the covered entity would still be required to notify individuals of a breach under state law, while they would be protected under the Federal law.

4. The Act's definition of "breach" provides for a variety of exceptions. To what particular types of circumstances do entities anticipate these exceptions applying?

The Privacy Rule recognizes that incidental disclosures are unavoidable and thus deems them as permitted disclosures. As with incidental disclosures, inadvertent uses and disclosures are a primary focus for all health care providers; however, even with heightened attention will happen to time to time, but are limited to the best degree possible.

Sincerely,

A handwritten signature in black ink, appearing to read "Bruce Yarwood". The signature is fluid and cursive, with a large, sweeping flourish at the end.

Bruce Yarwood
President and CEO