

2-HolmesHarmonLetters.pdf –

- Rea Holmes, Executive Assistant- letter dated May 7, 2008.....pages 1-2
- Tonya Harmon, CEO - email dated May 7, 2008..... pages 3-4
- Mike Lettman, Director of Information Security - email dated May 8, 2008page 5
- Kathy Johnson, Privacy Officer - email to Mike Lettman dated May 2, 2008.....pages 6-7



Jim Doyle, Governor
Karen E. Timberlake, Secretary

May 7, 2008

Fred Buhr
6112 Exchange Street
McFarland, WI 53558

Dear Mr. Buhr:

I am responding to your public records request and letter on behalf of Secretary Timberlake.

Enclosed, per your request, is a copy of the Department's current contract with Harmony Information Systems for SAMS, copies of agendas and minutes for the Nutrition Check Committee, copies of the agendas and minutes of the Data Stewardship Committee for the year 2000, and a list of subsequent Data Stewardship meetings.

We do not have a standard report on the number of nutrition participants' records contained in Wisconsin's SAMS servers. However, Karl Schlenker ran a query and determined that the total client count in question is approximately 163,744. Mr. Schlenker indicates that there is a significant but unknown quantity of duplicated client records in the database. Mr. Schlenker estimates that there are approximately 150,000 unduplicated clients with records in SAMS.

In your letter, as well as in a subsequent e-mail to me, you raise concerns about the security of the SAMS system and the use of the nutrition risk assessment.

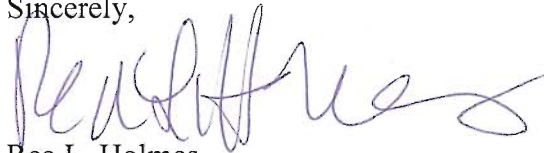
I have been assured that the specific security concern you raised has been fully addressed by Harmony Information Systems. I have also been advised that Harmony has been responsive to other security concerns that have been brought to their attention by Mr. Schlenker. Although I am aware of these reported potential risks to security, I am unaware of any actual breach of security (e.g., an actual inappropriate disclosure of confidential client information). Moreover, I was pleased to learn that Harmony will soon be conducting a third party audit. We look forward to reviewing the audit findings and recommendations.

Fred Buhr
May 7, 2008
Page Two

You also raise concerns about the use of the nutrition risk assessment. This was developed to meet federal requirements for nutrition screening. This screening tool helps assess whether or not individuals are at risk of poor nutrition and in need of services. The survey asks for information about known risk factors. Participation in the survey is voluntary. The Bureau of Aging and Disability Resources will be reviewing their training and resource materials to help insure that those who are using the assessment are appropriately telling clients that participation in the risk assessment is voluntary and that the information collected will be maintained in the client's electronic file.

I assure you that this Department takes its responsibility to protect client data very seriously. I will continue to work with the Bureau of Aging and Disability Resources to insure that information inputted into SAMS is secure.

Sincerely,

A handwritten signature in blue ink, appearing to read "Rea L. Holmes". The signature is fluid and cursive, with a long horizontal stroke at the end.

Rea L. Holmes
Executive Assistant

metasteward

From: fredbuhr@merr.com
Sent: Wednesday, May 07, 2008 7:12 PM
To: metasteward@metasteward.net
Subject: FW: Harmony

Original Message:

From: Tonya Harmon tharmon@harmonyis.com
Date: Wed, 7 May 2008 11:20:29 -0400
To: fredbuhr@merr.com
Subject: Harmony

Mr. Behr,

It has come to my attention that you continue to raise security concerns about our software to our customer, the State of Wisconsin, and to the media. I am surprised that you continue to have concerns given the repeated assurances you have received directly from our customer that these issues have been reviewed and addressed as appropriate.

Here at Harmony, we take the security of our software very seriously. If you have a concern about a particular security issue that you believe still exists, I would greatly appreciate that you contact me directly. To date, our company has never heard directly from you about any security issue. If you feel that your concerns have not been heard or addressed, I would be pleased to discuss them with you.

I am concerned, however, that you have some misinformation about our systems. I would like to address some specific factual inaccuracies in your latest email to our customer:

* Contrary to your assertion in your email to our client, Agingnetwork.com runs on Windows 2003, and has since its inception. At no time has it run on Windows 2000. It appears that your security concerns are based on an assumption about our operating system that is not correct. Since you stated in your email that had the system been running on Windows 2003 it would have been secure, I hope you now understand that it has been and is secure.

* You seem to be concerned that your concerns were not taken seriously. Let me assure you, that when your security queries were brought to the attention of the State, they quickly brought them to our attention, where they were treated very seriously. We understand that the State directly contacted you to assure you that the issues had been reviewed and addressed.

I would also ask you to be very careful as to what information you publicly disclose. Information that you may have had access to as an employee of the State of Wisconsin may be confidential information of the State or of Harmony and you likely have confidentiality

obligations regarding such information. We would also request that any statements that you do make about the Harmony system, be factually accurate. To date, they have not, and Harmony can not continue to allow such statements to go unchallenged.

We all want to make sure that Harmony software is secure. We believe it is, but to the extent you have factually accurate reasons to believe it is not, we are happy to hear from you. We are always assessing our systems to make sure that our security is where it needs to be to protect our client's information.

Regards,

Tonya Harmon

Tonya Harmon | CEO
P. 703.674.5101 | M. 703.628.3101 | Harmony <blocked::http://www.harmonyis.com/>
12120 Sunset Hills Rd. | Suite 500 | Reston, VA 20190

-----CONFIDENTIALITY
NOTICE-----

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain company confidential and privileged information.

Any unauthorized review, use, disclosure, or distribution is prohibited.

If you are not the intended recipient, please contact the sender by reply e-mail and destroy/delete all copies of the original message.

Email is not a secure form of communication.

Do not use email for storage or transmission of protected health information (PHI).

myhosting.com - Premium Microsoft® Windows® and Linux web and application hosting -
<http://link.myhosting.com/myhosting>

From: "Lettman, Mike J - DOA" <mike.lettman@wisconsin.gov>
To: fredbuhr@merr.com" <fredbuhr@rnerr.com>
Date: Thu, 8 May 2008 16:52:47 -0500
Subject: RE: Serious Security Problem

Hello Mr. Buhr

Thank you for your inquiry concerning security and privacy on DHFSBADR.org. The Dept of Health and Family Services (DHFS) and their vendor(s) are filly responsible for that particular site, application and the information it contains. We have forwarded your request to the DHFS and asked them to respond with answers to your questions.

Attached is a response from the DHFS. If you have any further security or privacy questions or concerns about this site you should raise those directly with the.DHFS.

DHFS has provided the following contact for you:

Kathy Johnson
DHFS Privacy Officer
608-266-5484
johnskl@dhfs.state.wi.us

Thanks again for contacting us concerning this matter.

Mike Lettman
Director of Information Security
Office of Security
Division of Enterprise Technology
Wisconsin, Department of Administration
P.O Box 7836
Madison, WI 53707-7836
Voice:(608) 224-3898

Response to Mike J. Lettman, DOA
DATE: May 2, 2008
RE: email from Fred Buhr April 30, 2008
SUBJECT: Alleged "Serious Security Problem"

Fred Buhr, a volunteer at the McFarland Senior Center, presents a series of assertions in this email which significantly misrepresent the conscientious administration of the Older Americans Act programs in the Bureau of Aging and Disability Resources (BADR) in DHFS. Staff in BADR has been respectful and attentive to Mr. Buhr's concerns for several months.

BADR has contracted with Area Agencies on Aging to secure the services of Karl Schlenker to administer the SAMS Older Americans program information system. Karl is supervised by an experienced manager in BADR. Policy memoranda, user guides, technical assistance and information about updates from the software provider (Harmony) are issued by BADR via email to all SAMS users. Karl is the primary author or distributor of the information

As a convenience to SAMS users, Karl set up an Internet site where he deposited the memos and material in response to frequently asked questions. The site includes training videos related to use of SAMS. All material is previously published and available from other sources. No secure or private personal information is presented on the site. The site was established without following protocol for DHFS web postings. The Bureau has begun transferring the SAMS information to the DHFS website, at which time the stand-alone website will be shut down. Harmony has not participated in the development or maintenance of the website. Further, Karl has not benefited in any way from managing this website, which is merely a repository of work materials for users.

- Mr. Buhr asserts that Karl is Harmony's sole administrator for SAMS in Wisconsin. This is not true. Karl is not a Harmony employee. Karl is Wisconsin's primary (but not sole) administrator for SAMS.
- Mr. Buhr asserts that Harmony provided Karl with a development environment to test Harmony's products. In fact, Karl declined the offer to participate.
- Mr. Buhr asserts that policy for the nutrition program has only been posted on Karl's internet site. This is not true. A manual of policies and procedures has been published by BADR.
- Mr. Buhr asserts that the Secretary has not approved content for the BADR Internet site as is required. The Secretary does not approve all web postings; this responsibility is delegated to the divisions. All material posted as policy was approved by management within the Division of Long Term Care/Bureau of Aging and Disability Resources.
- Mr. Buhr asserts that Harmony and BADR are one and the same. This is not true. The Bureau of Aging and Disability Resources is an agency within the Department of Health and Family Services, designated as the single state agency

on aging by the federal Administration on Aging. The Bureau has a contractual relationship with Harmony.

- Mr. Buhr asserts the every report listing participants by data entry operators is a breach of privacy for all persons listed in the report. This is not true. SAMS users can only see the names of individuals who are participants in their programs. County aging offices and their service providers are covered by the same confidentiality provisions that apply to all public human services programs.
- Mr. Buhr asserts that hundreds of thousands of individuals have had their privacy breached an astronomical number of times. This is not true. Repeated claims to that effect can only serve to falsely alarm senior citizens and should be vigorously denied.
- Mr. Buhr asserts that Harmony and BADR (DHFS) have not followed state laws or security standards and the SAMS system is vulnerable. We are aware of no violations of state law. Further, we expect that the forthcoming Third Party Security audit at Harmony will document the integrity of the system.
- Mr. Buhr asserts that his rights to serve as a data entry operator were revoked for a “poorly fabricated reason.” This is not true. Mr. Buhr informed Secretary Timberlake and Secretary Morgan in a correspondence received April 23, 2008, that he would suspend his data entry tasks as a volunteer because of his concerns about the SAMS system. Because he stated his intention to discontinue entering data, there is no need for him to maintain a password. Good security practice would suggest that when a staff member (or volunteer) resigns from his duties, his password should be revoked. Therefore, the password used by Mr. Buhr was changed as a standard security measure. This action was taken in consultation with McFarland Senior Center and Dane County.
- Mr. Buhr asserts that he and hundreds of thousands of Wisconsin’s citizens, and hundreds of millions nationwide have had their privacy breached countless times. We are not aware of any documented security breaches of SAMS.