



DEPARTMENT OF HEALTH AND HUMAN SERVICES  
OFFICE FOR CIVIL RIGHTS (OCR)



**HEALTH INFORMATION PRIVACY COMPLAINT**

|  |                     |  |  |
|--|---------------------|--|--|
| YOUR FIRST NAME<br><b>FREDERICK</b>                          |                     | YOUR LAST NAME<br><b>BUHR</b>                                    |  |
| HOME PHONE (Please include area code)<br><b>608.838.3946</b> |                     | WORK PHONE (Please include area code)                            |  |
| STREET ADDRESS<br><b>6112 EXCHANGE STREET</b>                |                     | CITY<br><b>McFARLAND</b>   |  |
| STATE<br><b>WI</b>   | ZIP<br><b>53558</b> | E-MAIL ADDRESS (if available)<br><b>FREDBUHR@METASTEWARD.NET</b> |  |

Are you filing this complaint for someone else?  Yes  No  
If Yes, whose health information privacy rights do you believe were violated?

FIRST NAME \_\_\_\_\_ LAST NAME \_\_\_\_\_

Who (or what agency or organization, e.g., provider, health plan) do you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule?  
PERSON / AGENCY / ORGANIZATION  
**PLEASE SEE ATTACHED**

|                |     |                                  |
|----------------|-----|----------------------------------|
| STREET ADDRESS |     | CITY                             |
| STATE          | ZIP | PHONE (Please include area code) |

When do you believe that the violation of health information privacy rights occurred?  
LIST DATE(S)  
**PLEASE SEE ATTACHED**

Describe briefly what happened. How and why do you believe your (or someone else's) health information privacy rights were violated, or the privacy rule otherwise was violated? Please be as specific as possible. (Attach additional pages as needed)  
**PLEASE SEE ATTACHED**

Please sign and date this complaint. You do not need to sign if submitting this form by email because submission by email represents your signature.

SIGNATURE **Frederick J. Buhr** DATE (mm/dd/yyyy) **03/27/2010**

Filing a complaint with OCR is voluntary. However, without the information requested above, OCR may be unable to proceed with your complaint. We collect this information under authority of the Privacy Rule issued pursuant to the Health Insurance Portability and Accountability Act of 1996. We will use the information you provide to determine if we have jurisdiction and, if so, how we will process your complaint. Information submitted on this form is treated confidentially and is protected under the provisions of the Privacy Act of 1974. Names or other identifying information about individuals are disclosed when it is necessary for investigation of possible health information privacy violations, for internal systems operations, or for routine uses, which include disclosure of information outside the Department for purposes associated with health information privacy compliance and as permitted by law. It is illegal for a covered entity to intimidate, threaten, coerce, discriminate or retaliate against you for filing this complaint or for taking any other action to enforce your rights under the Privacy Rule. You are not required to use this form. You also may write a letter or submit a complaint electronically with the same information. To submit an electronic complaint, go to OCR's Web site at: [www.hhs.gov/ocr/privacy/hipaa/complaints/index.html](http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html). To mail a complaint see reverse page for OCR Regional addresses.

The remaining information on this form is optional. Failure to answer these voluntary questions will not affect OCR's decision to process your complaint.

Do you need special accommodations for OCR to communicate with you about this complaint? (Check all that apply)

- Braille   
  Large Print   
  Cassette tape   
  Computer diskette   
  Electronic mail   
  TDD  
 Sign language interpreter (specify language): \_\_\_\_\_  
 Foreign language interpreter (specify language): \_\_\_\_\_   
 Other: \_\_\_\_\_

If we cannot reach you directly, is there someone we can contact to help us reach you?

|                                       |     |                                       |  |
|---------------------------------------|-----|---------------------------------------|--|
| FIRST NAME                            |     | LAST NAME                             |  |
| HOME PHONE (Please include area code) |     | WORK PHONE (Please include area code) |  |
| STREET ADDRESS                        |     | CITY                                  |  |
| STATE                                 | ZIP | E-MAIL ADDRESS (If available)         |  |

Have you filed your complaint anywhere else? If so, please provide the following. (Attach additional pages as needed)

PERSON / AGENCY / ORGANIZATION / COURT NAME(S)

*PLEASE SEE ATTACHED*

|               |                           |
|---------------|---------------------------|
| DATE(S) FILED | CASE NUMBER(S) (If known) |
|---------------|---------------------------|

To help us better serve the public, please provide the following information for the person you believe had their health information privacy rights violated (you or the person on whose behalf you are filing).

ETHNICITY (select one)      RACE (select one or more)

Hispanic or Latino   
  American Indian or Alaska Native   
 Asian   
 Native Hawaiian or Other Pacific Islander  
 Not Hispanic or Latino   
 Black or African American   
 White   
 Other (specify): \_\_\_\_\_  
 PRIMARY LANGUAGE SPOKEN (if other than English) \_\_\_\_\_

How did you learn about the Office for Civil Rights?

- HHS Website/Internet Search   
 Family/Friend/Associate   
 Religious/Community Org   
 Lawyer/Legal Org   
 Phone Directory   
 Employer  
 Fed/State/Local Gov   
 Healthcare Provider/Health Plan   
 Conference/OCR Brochure   
 Other (specify): \_\_\_\_\_

To mail a complaint, please type or print, and return completed complaint to the OCR Regional Address based on the region where the alleged violation took place. If you need assistance completing this form, contact the appropriate region listed below.

|   |  |   |
|---|--|---|
| <b>Region I - CT, ME, MA, NH, RI, VT</b><br>Office for Civil Rights, DHHS<br>JFK Federal Building - Room 1875<br>Boston, MA 02203<br>(617) 565-1340; (617) 565-1343 (TDD)<br>(617) 565-3809 FAX                       | <b>Region V - IL, IN, MI, MN, OH, WI</b><br>Office for Civil Rights, DHHS<br>233 N. Michigan Ave. - Suite 240<br>Chicago, IL 60601<br>(312) 886-2359; (312) 353-5693 (TDD)<br>(312) 886-1807 FAX | <b>Region IX - AZ, CA, HI, NV, AS, GU, The U.S. Affiliated Pacific Island Jurisdictions</b><br>Office for Civil Rights, DHHS<br>90 7th Street, Suite 4-100<br>San Francisco, CA 94103<br>(415) 437-8310; (415) 437-8311 (TDD)<br>(415) 437-8329 FAX |
| <b>Region II - NJ, NY, PR, VI</b><br>Office for Civil Rights, DHHS<br>26 Federal Plaza - Suite 3313<br>New York, NY 10278<br>(212) 264-3313; (212) 264-2355 (TDD)<br>(212) 264-3039 FAX                               | <b>Region VI - AR, LA, NM, OK, TX</b><br>Office for Civil Rights, DHHS<br>1301 Young Street - Suite 1169<br>Dallas, TX 75202<br>(214) 767-4056; (214) 767-8940 (TDD)<br>(214) 767-0432 FAX       |   |
| <b>Region III - DE, DC, MD, PA, VA, WV</b><br>Office for Civil Rights, DHHS<br>150 S. Independence Mall West - Suite 372<br>Philadelphia, PA 19106-3499<br>(215) 861-4441; (215) 861-4440 (TDD)<br>(215) 861-4431 FAX | <b>Region VII - IA, KS, MO, NE</b><br>Office for Civil Rights, DHHS<br>601 East 12th Street - Room 248<br>Kansas City, MO 64106<br>(816) 426-7277; (816) 426-7065 (TDD)<br>(816) 426-3686 FAX    |   |
| <b>Region IV - AL, FL, GA, KY, MS, NC, SC, TN</b><br>Office for Civil Rights, DHHS<br>61 Forsyth Street, SW. - Suite 3B70<br>Atlanta, GA 30303-8909<br>(404) 562-7886; (404) 331-2867 (TDD)<br>(404) 562-7881 FAX     | <b>Region VIII - CO, MT, ND, SD, UT, WY</b><br>Office for Civil Rights, DHHS<br>1961 Stout Street - Room 1426<br>Denver, CO 80294<br>(303) 844-2024; (303) 844-3439 (TDD)<br>(303) 844-2025 FAX  | <b>Region X - AK, ID, OR, WA</b><br>Office for Civil Rights, DHHS<br>2201 Sixth Avenue - Mail Stop RX-11<br>Seattle, WA 98121<br>(206) 615-2290; (206) 615-2296 (TDD)<br>(206) 615-2297 FAX   |

**Burden Statement**

Public reporting burden for the collection of information on this complaint form is estimated to average 45 minutes per response, including the time for reviewing instructions, gathering the data needed and entering and reviewing the information on the completed complaint form. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: HHS/OS Reports Clearance Officer, Office of Information Resources Management, 200 Independence Ave. S.W., Room 531H, Washington, D.C. 20201. **Please do not mail this complaint form to this address.**

HHS-700 (7/09) (BACK)



## COMPLAINANT CONSENT FORM

The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) has the authority to collect and receive material and information about you, including personnel and medical records, which are relevant to its investigation of your complaint.

To investigate your complaint, OCR may need to reveal your identity or identifying information about you to persons at the entity or agency under investigation or to other persons, agencies, or entities.

The Privacy Act of 1974 protects certain federal records that contain personally identifiable information about you and, with your consent, allows OCR to use your name or other personal information, if necessary, to investigate your complaint.

Consent is voluntary, and it is not always needed in order to investigate your complaint; however, failure to give consent is likely to impede the investigation of your complaint and may result in the closure of your case.

Additionally, OCR may disclose information, including medical records and other personal information, which it has gathered during the course of its investigation in order to comply with a request under the Freedom of Information Act (FOIA) and may refer your complaint to another appropriate agency.

Under FOIA, OCR may be required to release information regarding the investigation of your complaint; however, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

Please read and review the documents entitled, *Notice to Complainants and Other Individuals Asked to Supply Information to the Office for Civil Rights and Protecting Personal Information in Complaint Investigations* for further information regarding how OCR may obtain, use, and disclose your information while investigating your complaint.

**In order to expedite the investigation of your complaint if it is accepted by OCR, please read, sign, and return one copy of this consent form to OCR with your complaint. Please make one copy for your records.**

- As a complainant, I understand that in the course of the investigation of my complaint it may become necessary for OCR to reveal my identity or identifying information about me to persons at the entity or agency under investigation or to other persons, agencies, or entities.



- I am also aware of the obligations of OCR to honor requests under the Freedom of Information Act (FOIA). I understand that it may be necessary for OCR to disclose information, including personally identifying information, which it has gathered as part of its investigation of my complaint.
- In addition, I understand that as a complainant I am covered by the Department of Health and Human Services' (HHS) regulations which protect any individual from being intimidated, threatened, coerced, retaliated against, or discriminated against because he/she has made a complaint, testified, assisted, or participated in any manner in any mediation, investigation, hearing, proceeding, or other part of HHS' investigation, conciliation, or enforcement process.

**After reading the above information, please check ONLY ONE of the following boxes:**

**CONSENT:** I have read, understand, and agree to the above and give permission to OCR to reveal my identity or identifying information about me in my case file to persons at the entity or agency under investigation or to other relevant persons, agencies, or entities during any part of HHS' investigation, conciliation, or enforcement process.

**CONSENT DENIED:** I have read and I understand the above and do not give permission to OCR to reveal my identity or identifying information about me. I understand that this denial of consent is likely to impede the investigation of my complaint and may result in closure of the investigation.

Signature: Frederick J. Buhr Date: 03/27/2010  
\*Please sign and date this complaint. You do not need to sign if submitting this form by email because submission by email represents your signature.

Name (Please print): FREDERICK J. BUHR

Address: 6192 EXCHANGE ST.  
McFARLAND, WI 53558

Telephone Number: 608.838.3946

**Department of Health and Human Services  
Office for Civil Rights (OCR)  
Health Information Privacy and Security Complaint**

**Complainants:**

Frederick J. Buhr  
(registered agent for)  
Metasteward LLC  
6112 Exchange Street  
McFarland, WI 53558  
608.838.3946  
fredbuhr@metasteward.net

I am filing this complaint on behalf of myself and (as the registered agent) on behalf of Metasteward LLC concerning systemic omissions and violations of HIPAA privacy and security rules by the following named entities: U.S. Administration on Aging (AoA), Wisconsin Bureau of Aging and Disability Resources (BADR), Dane County Area Agency on Aging (AAA) and Harmony Information Systems (formerly Synergy Technologies). The violations of HIPAA rules affect me and all consumers whose medical information is collected and stored in the Social Assistance Management System (SAMS) hosted on Harmony Information Systems' Internet site: <http://AgingNetwork.com>.

**Dates When Violations Occurred:**

Violations of the fundamental concept of *informed consent* included in "Fair Information Practices"<sup>1</sup> (the foundation of HIPAA requirements) occurred at the outset of Wisconsin's contract to license the SAMS program in 2001. HIPAA omissions and violations by the named entities are (in my opinion) systemic to the entire U.S. Aging Network and appear to have been occurring since the effective dates of the Privacy and Security Rules. A management information study prepared for the National Association of State Units on Aging in 2006 found that only 57 percent of the state units on aging (SUAs) reported that their information systems were compliant with HIPAA confidentiality requirements.<sup>2</sup> I became aware of Dane County AAA's and BADR's (Wisconsin's SUA) ongoing privacy violations in January 2008 and security violations in February 2008. In May 2008 I received correspondence from BADR and Harmony Inc. (vendor of SAMS) which I considered threatening and retaliatory in nature in violation of HIPAA requirements to not threaten or retaliate.

On March 7, 2008 I met with Dane County and DHFS nutrition specialists and explained my concerns related to violations of privacy of the electronic health records in SAMS. On April 7, 2008 I explained and provided documentation of my concerns to DHFS senior security administrators in a meeting<sup>3</sup> and received assurances that my concerns would be passed on to the Department's HIPAA privacy officer.<sup>4</sup> On April 21, 2008 I sent a letter to the Secretaries of the Department of Health and Family Services and Department of Administration with copies to the ACLU and the Associated Press<sup>5</sup> raising concerns that federal and state laws<sup>6</sup> were being circumvented<sup>7</sup>. On April 30, 2008 I sent an email to the State's chief security officer regarding

my discovery that the website at: <http://dhfsbadr.org/index> was not State owned but rather was privately owned by Wisconsin's SAMS administrator.<sup>8</sup>

In my opinion, responses to my complaints, when taken either singly or together, constitute egregious violations of my rights under HIPAA to be assured that I will not be threatened or retaliated against for filing complaints. The first response I received was on May 7, 2008 from Tonya Harmon, CEO of Harmony Inc. which I considered to be threatening.<sup>9</sup> The second from Wisconsin's HIPAA privacy officer, forwarded to me by the State's chief security officer, was retaliatory in nature.<sup>10</sup>

Furthermore, systemic omissions and violations concerning implementation of changes to HIPAA under the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) have been occurring in Wisconsin since passage of the Act in February 2009 and include omissions and violations of provisions of that Act which became effective on February 17, 2010.

### **Names of Entities Violating Health Information Privacy and Security Rules:**

U.S. Administration on Aging (AoA)  
Department of Health and Human Services  
One Massachusetts Avenue  
Washington, DC 20201  
202.401.4634

Bureau of Aging and Disability Resources (BADR)  
Wisconsin Department of Health Services (DHS)  
1 West Wilson Street  
Madison, WI 53702  
608.266.1865

Dane County Area Agency on Aging (AAA)  
2322 South Park Street  
Madison, WI 53713  
608.261.9930

Harmony Information Systems  
Suit 500  
12120 Sunset Hills Road  
Reston, VA 201960  
703.628.3101

### **Summary of Complaint:**

The proprietary site: <http://agingnetwork.com> connects (through both human and Internet interfaces) many local managed care organizations (MCOs) and aging and disability resources centers (ADRCs) to State of Wisconsin databases (containing personally identifiable health

related data) including but not limited to: the Human Services Reporting System (HSRS); the Client Assistance for Reemployment and Economic Support (CARES); Wisconsin Incident Tracking System (WITS); Functional Screen Information Access (FSIA); Family Care; Data Warehouse (DW) and the ForwardHealth interchange, Wisconsin's Medicaid Management Information System (MMIS). The ForwardHealth Portal<sup>11</sup> is used by managed care organizations, providers, partners and trading partners throughout the State to submit, manage, and maintain health records for members under their care.

The privacy and security of protected health information of many individuals maintained in State systems is violated by systemic transfer of protected information to databases hosted on Harmony Inc.'s servers and accessed over the Internet. Harmony indicates on its website that agencies can achieve full HIPAA compliance for all their databases by utilizing Harmony's systems<sup>12</sup> which is not true.

Harmony's flagship application SAMS appears to be the de facto federal information system for the Administration on Aging by virtue of participation by AoA staff and administrators in Harmony's user conferences.<sup>13</sup> The Dane County Area Agency on Aging (AAA) at the direction of the Bureau of Disability Resources (BADR) utilizes the Social Assistance Management System (SAMS) hosted on AgingNetwork.com (owned by Harmony) without fully informing me (and others) of our rights under HIPAA's Privacy Rule, fails to protect our medical information as required under HIPAA's Security Rule and threatens and retaliates against me in response to my complaints.

In lieu of a Notice of Privacy Practices (NPP) BADR requires aging units and their providers to include the following "privacy statement" on all registration forms, nutrition risk forms, and any other forms used to collect client specific information that is placed in the SAMS database.

*"The information you are being asked to provide is needed to determine if you are eligible to receive Older Americans Act Services and to comply with federal reporting requirements. This information will be stored in a secure electronic database and will not be used for any other purpose. Your information will not be shared with another agency without your permission. This information will not be sold to anyone. You have the right to review your electronic record and request changes to assure accuracy. You will not be denied most services if you refuse to provide this information. If you have questions regarding this, please ask the aging unit staff."*<sup>14</sup>

The protected health information (PHI) of any person is viewable on the SAMS summary screen of the person's electronic record. Whenever a data entry operator attempts to enter information concerning a new participant, summary screens of all persons having similar last names are listed and can be accessed without actually opening the person's record. The visible fields on the summary screens include personal identifiers and protected health information including health risk assessments and diagnoses.<sup>15</sup> For those instances where an individual declines to supply information, data entry operators have been instructed to "overload" one of the fields with XXXs. There is no indication of compliance with HIPAA's Security Rule nor is there any evidence that an audit trail log is maintained as to who views records.

The protected health information that I and others have been asked to provide as participants in the congregate meals program greatly exceeds the basic eligibility factor of age (being over 60). Further the requirement to clearly specify a HIPAA complaint process to be followed with a named HIPAA privacy officer and address and the right to appeal to the federal Department of Health and Human Services without fear of threats or retaliation is not followed.

### **Systemic Violations due to Accidental Enterprise Architectures:**

From 1998 until 2005, when the Center for Uniformity and Security (CUSP) was disbanded due to budget constraints, I held the position of in-house data administration consultant for the (then) Department of Health and Family Services (DHFS). CUSP's mission was driven by two federal laws that were enacted in 1996. The first was the *Clinger-Cohen Act* having to do with the *Federal Enterprise Architecture (FEA)* and the second was the *Health Insurance Portability and Accountability Act (HIPAA)*.

During that period, I participated in HIPAA standards development as a public sector representative to Health Level 7 (HL7) and as a participant in the HIPAA Metadata Registry Coalition and United States Healthcare Information Knowledgebase (USHIK). I was a beta tester of MetaPro sponsored by the Environmental Protection Agency (EPA) and the (then) Health Care Financing Administration (HCFA). MetaPro was a distributable metadata registry based on the *ANSI X3.825 Metamodel for the Management of Sharable Data* and *ISO/IEC 11179 Specification and Standardization of Data Elements*. I was the eforms coordinator for the Department and the primary staff person for the Department's Data Stewardship Council and principle author of the Common Core Data Standards that the Council adopted. I maintained the HIPAA Website<sup>16</sup> for the Department and provided consultation to IT projects on data security, privacy, and quality. I consulted with the Department's units administering Medicaid and social services as to the proper placement of social services in the Health Care Provider Taxonomy<sup>17</sup>

Since 2006, as an independent data administration consultant representing the consumer sector, I have been both an observer and participant on the Health Information Technology Standards Panel (HITSP) and its technical committees and currently am a member of the HL7 working group on personal health records (PHRs). HITSP is a cooperative partnership between public and private sectors. The Panel was created in order to harmonize and integrate standards that will meet clinical and business needs for sharing information. HITSP technical committees also identify gaps in standards and turn to standards development organizations to develop those missing standards. HL7 is a standards development organization (SDO) that develops standards where none currently exist. I currently participate on the HL7 personal health records (PHRs) workgroup.

Enterprise architecture is a relatively new discipline having its origins in an article John Zachman (founder of Zachman International) published in 1987 describing what is now known as the *Zachman Framework*™. It is this framework that is the basis for the Federal Enterprise Architecture. Every organization has an *enterprise architecture*. Built into the concept of enterprise architecture is the idea that organizations are systems that involve people, rules, processes, and technology. Another area that deserves attention is the notion of components. Fundamental to understanding enterprise architecture is learning to view the separate pieces of

the organization and technology system that form the enterprise. It is important to understand the conceptual difference between a *system of records* and the *records themselves* that are contained in the system.

I have closely followed information exchange (IE) technology at state and national levels as it relates specifically to healthcare information exchange (HIE) and more broadly to information exchange itself at the national level through the National Information Exchange Model (NIEM). In August 2007, during a period when I was examining the enterprise architecture of the Village of McFarland (Wisconsin),<sup>18</sup> I volunteered to enter data for the McFarland Senior Outreach Program relating to the Older Americans Act nutrition programs. I was trained on the Social Assistance Management System (SAMS) by the previous data entry operator and studied materials that were available on the dhfsbadr.org site including all presentations of the 2007 SAMS user conference.<sup>6</sup>

The Village of McFarland has mix of systems, processes, applications, data, people, committees and an IT infrastructure that is combined in some manner to have all pieces work together — or not work together — as its enterprise architecture. In the heading to this section, I refer to this as an “*Accidental Enterprise Architecture*”. Of all the systems and databases I studied in McFarland, SAMS (mandated and paid for by Dane County and the State of Wisconsin) was the most ill suited for its intended use as a system related to persons who only participate in the congregate and home delivered meal programs of McFarland’s Senior Outreach Program. McFarland’s program for seniors is based on a social-services model of services. SAMS is (as advertised) designed for reporting on Home and Community Based Waiver programs (HCBW) and is based on a medical model.

While I didn’t realize it at the time, a site visit examining community based long-term care by the National Health Policy Forum was taking place in Wisconsin during August 2007. The George Washington University of Washington D.C. issued a report on the site visit on December 14, 2007.<sup>19</sup> The report provides a clear description of the differences between a medical model and a social-services model and indicates that a compromise was reached between the two factions resulting in a program: *Family Care* that would only integrate long-term care services using a person centric approach. Although the Bureau of Aging and Disability Resources (BADR) had selected the web-based version of SAMS in 2005 to consolidate data at the State level that previously had been collected and maintained at the local level, no mention of the statewide system was made to the site visit participants from the National Health Policy Forum. On page 13 of the Health Policy Forum’s report it was noted that the site visitors were surprised to find, in a sophisticated social services environment, so little mention of electronic record keeping.

My background is that of a social worker from the 1960’s. In the early 1970’s I was the principle author of Wisconsin’s *County Plans for Social Services*. The social services system at that time was state-supervised county-administered. A number of services including congregate and home delivered meals and information and referral services were not to be means tested and case records were not to be opened on the participants. At that point in time, scores on health risk assessments and functional evaluations related to activities of daily living (ADLs) and instrumental activities of daily living (IADLs) were not considered as factors of eligibility for

social services. The scores of individuals' personal assessments of their ADLs and IADLs are entered into SAMS based upon individuals' personal perceptions without instructions on how to complete the assessments. This is in contrast to training provided on how to complete similar assessments for the Functional Screen offered to professionals with a requirement that a test be passed in order to administer the assessments.<sup>20</sup>

So today, I find it an invasion of my rights to privacy to have an electronic health record opened on me (without asking for my permission) and others if we only want to participate in a congregate meal for social reasons and voluntarily pay for the full cost of the meal. I find it an egregious invasion of privacy that electronic health records are opened on individuals and that fields are populated with information from other databases when an individual only requests information about programs such as Medicare, Social Security, Senior Care, FoodShare and other benefit programs. Yet over the weekend of March 5 through March 7, 2010 personal health care information was migrated from Harmony's Beacon Information and Assistance (I&A) application into Wisconsin's statewide SAMS database<sup>21</sup> without asking permission of clients or consumers or members of managed care organizations (MCOs).

I'll explain why I find the migration of health information from other databases so egregious by using a group five fields labeled: Diagnosis1, Diagnosis2, Diagnosis3, Diagnosis4, and Diagnosis5 located on the SAMS Summary Screen.<sup>13</sup> The grouping of five fields is a distinctive pattern related to the multi-axial diagnostic system of the Diagnostic and Statistical Manual (DSM) of mental disorders. I believe that these fields relate to five fields identified in the Human Services Reporting System (HSRS) Mental Health Module<sup>22</sup> in *Section 12 Diagnostic Impression* as well as five fields recorded in Section 2 of the ForwardHealth Outpatient Mental Health Assessment form<sup>23</sup> and five fields in the Departments Data Warehouse database. ForwardHealth provides instructions<sup>24</sup> as to how to complete the outpatient mental health assessment and treatment plan forms.

It is possible that one person's mental health diagnosis can appear in each of four databases as five fields.

- Axis I is reserved for clinical disorders – for example a *panic disorder*
- Axis II is for personality disorders – for example a *histrionic personality disorder*
- Axis III is for medical and/or physical conditions or disorders – for example *hyperthyroidism*
- Axis IV indicates factors contributing to, or affecting the current psychiatric disorder and treatment outcomes – for example *social issues*
- Axis V is for the global assessment functioning (GAF). This is a 100 point scale used to describe the patient's overall level of performance in usual daily activities and social, occupational, academic and interpersonal functioning.

In 2002 I developed a data quality protocol as part of the Data Infrastructure Grant (DIG) designed to measure the quality of data being passed from the HSRS Mental Health Module to corresponding fields in the Department's Data Warehouse (DW). I analyzed in detail the five diagnostic fields of over 130,000 records. My suspicion is that staff having access to the data warehouse are transferring the information to an individual's SAMS electronic record without informing the individual. There is no indication that consumers have given their informed

consent or that HIPAA rules relating to security are followed. Information that is recorded on individuals' summary screens is accessible without any indication that an audit tracking log is in place.

User fields on the SAMS summary screen are also utilized to record medical information of individuals participating in the Stanford Chronic Disease Self Management Program (CDSMP) and the Family Care Giver Support Program (FCSP).<sup>14</sup> The user fields contain a choice of values: Don't Know, No and Yes and are identified by the following chronic disease labels: lw1-Diabetes; lw2-HeartDisease; lw3-Hypertension; lw4-LungDisease; lw5-Depression; lw6-ArthritisRheum; lw7-Cancer and lw8-OtherChronic. CDSMP is a 17-hour course taught by lay people who teach individuals how to manage their symptoms and maintain functional ability.

On the screen print of the SAMS (demo) summary screen I have drawn particular attention to the user field labeled *Depression* which is one of the chronic diseases identified in the Living Well program. As I have mentioned earlier, I am a member of the U.S. Health Information Technology Standards Panel (HITSP) and have closely followed deliberations (via teleconference) of the two federal advisory committees (FACAs) established under the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). At times I have spoken directly to the committees when the phone lines were opened for public comment.

On August 14, 2009 during the public comment portion of the Health Information Technology (HIT) Policy Committee meeting, I heard Dr. Deborah Peel, who is a psychiatrist and founder of *Patients Privacy Rights* (a consumers advocacy organization) say she feared her coalition's written concerns, representing more than 10 million Americans were never considered by the committee. Dr. Peel mentioned the fear individuals have concerning breaches of privacy in their health care records and that depression was one of the leading medical causes of disability. She said that if we have a system of electronic records that does not allow trust and segmentation of mental health information, we will never get that data because people will not divulge it. She went on to say that we know from the federal Department of Health and Human Services' own findings that two million people a year refuse to get treatment for mental illness because they know that their medical information it is not kept private. Six hundred thousand people refuse early diagnosis and treatment of cancer because they know the information will not be kept private.<sup>25</sup>

Wisconsin's implementation of SAMS is programmed so as to breach the privacy of all persons whose medical information is entered into the system. My nutrition risk assessment information has been entered into the SAMS system and I believe that my privacy rights have been breached. I evaluate the privacy and security of electronic records systems which hold my own health information from the standpoint of a technical expert. I can't imagine a less secure and less private system than SAMS. During the public comment portion of the May 15, 2009 HIT Standards Committee Meeting,<sup>26</sup> I told of my work related to HIPAA as a former employee of DHFS (now DHS). I went on to volunteer to provide feedback to the Committee as a real live volunteer "use case." My own experience with SAMS prompts my privacy and security complaint. I followed my offer to be a "volunteer use case" with an email to the Office of the National Coordinator (ONC) in which I mentioned that my experiences with the administrators in Wisconsin's Department of Health Services were so disappointing that I intended "to pursue

remediation of what I feel are egregious privacy and security violations being committed by Wisconsin's Department of Health Services (DHS)."<sup>27</sup> The accidental enterprise architecture of the Wisconsin Department of Health Services (DHS) jeopardizes the entire healthcare information interchange efforts of the State, not only for the present, but for the future as well.

As I mentioned earlier in my complaint, on April 21, 2008 I sent a letter to DHFS Secretary Karen Timberlake and DOA Secretary Michael Morgan<sup>7</sup> recommending that the eHealth Care Quality and Patient Safety Board consider a law prohibiting State and local agencies from circumventing HIPAA and state administrative rules relating to transmitting and storing personally identifiable information in electronic databases outside the State's firewalls. I recommended that the Department move all records in SAMS to the HSRS database (which is inside the State's firewalls).

Karen Timberlake was chairperson and Michael Morgan a member of the eHealth Board that Governor Jim Doyle established by executive order on November 2, 2005. I view the eHealth Board as the forerunner of the federal advisory committees ( FACAs) created by the HITECH Act of 2009. Appointed members of the board included representatives (to name only a few) from: Epic Systems Corporation, Microsoft, GE Healthcare, Marshfield Clinic, Symphony Corporation and Metavante Corporation.

My letter to Secretaries Timberlake and Morgan followed a letter dated April 15, 2008 from Governor Doyle to Secretary Morgan sharing the release of a privacy assessment by Metavante Corporation. Governor Doyle had requested that the privacy assessment be conducted after two major security breaches, involving social security numbers being visible on address labels, occurred in January 2008.<sup>28</sup> Metavante (a member of the board) told the Governor that although it had found that the state's agencies already had some strong policies and practices in place for protecting sensitive information further steps could be taken to make the systems even more secure. Unfortunately the study was flawed in that it only included databases contained *inside* Wisconsin's network firewalls, not those bypassing the state's firewalls by transmitting sensitive information directly over the Internet to networks hosted on servers *outside* the state's firewalls.

The Social Assistance Management System (SAMS) hosted on <http://agingnetwork.com> (the system of concern in my complaint) was not included among the systems that were assessed. Effective December 1, 2009, the eHealth Care Quality and Patient Safety Board was sunset by Executive Order 303 and the new Wisconsin Relay of Electronic Data (WIRED) for Health Board was established to govern statewide health information exchange planning and implementation. The old eHealth Board was dissolved without the issues addressed in my complaint being brought before it.

On February 23, 2010 Governor Doyle announced members of the new WIRED for Health Board. A number of the major companies that had been on the previous board (Epic Information Systems, GE Healthcare, Microsoft, Symphony and Metavante) were not appointed to the new board. I believe it was a fundamental mistake to abandon five years of work coming from the old eHealth Board which was (in my opinion) the world's most credentialed board. The HIPAA security and privacy issues that I identified in my April 14, 2008 letter remain and must be recognized when planning for the future statewide health information exchange.

Wisconsin is slated to receive \$9.44 million from ONC this year to plan for health information exchanges. Wisconsin expects, over the next few years, to receive over \$80 million for HIE implementation projects. A request for information (RFI) for a Long-term Managed Care Infrastructure HIE project that will integrate all legacy long-term care systems, vital records and Wisconsin's data warehouse was released in August 2009.<sup>29</sup> DHS has indicated that it will likely release a request for proposal (RFP) for the infrastructure project in the second half of 2010.

Metasteward LLC would have responded to the request for information (RFI) 1682-RFI-PM were it not for the fact that in May 2008 I received correspondence from BADR and Harmony Inc. (vendor of SAMS) which I considered threatening and retaliatory in nature, in violation of HIPAA requirements to not threaten or retaliate. Harmony Inc. is one of the vendors who attended the vendor's Q&A webinar<sup>30</sup> and individuals from BADR staff are among those who are reviewing the submissions.

### **In Summary:**

In summary, I believe that my privacy rights as an individual and Metasteward LLC's rights as a company to participate in a fair and impartial procurement process have been violated. Even my right to volunteer as a consumer technical expert on a WIRED for Health workgroup has been violated by the hostile communications from Wisconsin's chief of security and the DHS HIPAA privacy officer.<sup>10</sup>

I have served on a number of HITSP committees and workgroups including the Consumer Preferences Tiger Team which reported directly to the ONC reviewing the *Consumer Preferences Draft Requirements Document*. When that document was released for public input, I sent an email to the project manager of the RFI informing him of the opportunity for DHS to comment.<sup>31</sup>

I hope that the Office of Civil Rights (OCR) will take my complaints seriously. I believe that health information exchanges (at both the state and national levels) have been and will continue to be compromised unless the issues related to the information systems of the Older Americans Act programs are resolved.

After nearly two and a half years since I discovered the security and privacy breaches, I am exasperated that they still exist. I assumed that once the problems were pointed out swift measures would be taken to remedy and solve the problems. I thought that Governor Doyle, once informed of the problems, would contact former Governor Thompson (who was on Harmony's board of directors) and that they would quietly have the system taken off-line and fixed.

Rather than that happening, the SAMS administrator told me that he had already known of the problems that I found and that the problems had been resolved.<sup>32</sup> The security and privacy issues of Internet hosted applications such as <http://agingnetwork.com> are so complex that they require professional risk assessments, not only of applications running on the host and client systems, but of the transmission layers of the Internet itself.

In closing, I believe that the security and privacy of millions of the most vulnerable individuals has been breached innumerable times due to the failures in exercising due diligence by the following entities: the U.S. Administration on Aging (AoA); the Wisconsin DHS/Bureau of Aging and Disability Resources (BADR); the Dane County Area Agency on Aging (AAA) and Harmony Information Systems.

## End Notes

<sup>1</sup> *Model Standards of Fair Information Practices*; A basic history of fair information practices can be found at: <http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>

<sup>2</sup> Copy of title page and pages 17, 23 and 35 of the *State Aging Information Systems Management Study* prepared for the National Association of State Units on Aging by Westat: December 2006

<sup>3</sup> Agenda for meeting with Chuck Crawford Committee – April 7, 2008; 9:00 A.M.

<sup>4</sup> Copy of email from Charles Crawford acknowledging my complaints dated 4/7/2008

<sup>5</sup> Article by Scott Bauer, Associated Press at: [http://www.phiprivacy.net/documentation/2008/WiDHFS\\_02.html](http://www.phiprivacy.net/documentation/2008/WiDHFS_02.html) accessed on 03/07/2010

<sup>6</sup> Wisconsin has the strongest laws in the nation relating to forms and records containing personally identifiable information. A specific rule (ADM 12) relates to electronic records. Instructions concerning records retention and destruction can be viewed at: <http://www.doa.state.wi.us/docview.asp?docid=8070&locid=2>

<sup>7</sup> Copy of letter to Secretaries Timberlake and Morgan dated 4/21/2008

<sup>8</sup> Email to Mike Lettman regarding dhfsbadr.org website being privately owned

<sup>9</sup> Email response from Tonya Harmon, CEO of Harmony Inc. dated 5/7/2008

<sup>10</sup> Email response from Mike Lettman and DHFS response from Kathy Johnson, HIPAA Privacy Officer

<sup>11</sup> Pages 7, 10, 12 and 41 of Long Term Care Data Warehouse instructions accessed on 03/07/2010 at:

[http://dhs.wi.gov/lcaredatawarehouse/documents/LTCDW\\_User\\_Guide\\_v\\_1\\_2.pdf](http://dhs.wi.gov/lcaredatawarehouse/documents/LTCDW_User_Guide_v_1_2.pdf)

<sup>12</sup> Screen print of website: <http://agingnetwork.com> accessed on 02/25/2010

<sup>13</sup> Screen print of Harmony News related to Harmony User's 2008 Conference accessed on 2/26/2010

<sup>14</sup> Communication from BADR to all aging units dated 07/15/2008

<sup>15</sup> Screen print of SAMS summary screen of "demo" record accessed on 11/15/2009

<sup>16</sup> The original HIPAA Now! home page that I maintained can still be viewed at: <http://dhs.wi.gov/hipaa/index.htm> .

An updated resource page including links to HITECH provisions is available at:

<http://dhs.wi.gov/hipaa/resources/resources.htm> . Both pages were accessed on 03/08/2010.

<sup>17</sup> Cover and table of contents for the 2008 Health Care Provider Taxonomy; Social services provided by managed care organizations (MCOs) and nursing or custodial care facilities are clearly subject to HIPAA rules while social services provided through a strictly social services model agency might not be subject to HIPAA.

<sup>18</sup> Minutes of the December 18, 2007 Communications and Technology Committee summarizing my presentation on the National Information Exchange Model (NIEM) can be viewed at:

[http://www.mcfarland.wi.us/DesktopModules/Bring2mind/DMX/Download.aspx?TabId=547&DMXModule=1369&Command=Core\\_Download&EntryId=1484&PortalId=0](http://www.mcfarland.wi.us/DesktopModules/Bring2mind/DMX/Download.aspx?TabId=547&DMXModule=1369&Command=Core_Download&EntryId=1484&PortalId=0)

The home page of the National Information Model can be viewed at: <http://www.niem.gov/>. Both sites were accessed on 03/09/2010.

<sup>19</sup> National Health Policy Forum Site Visit – Wisconsin August 8-1-, 2007; cover and pages 12,13 and 20; entire report can be viewed at: [http://www.nhpf.org/library/site-visits/SV\\_Wisconsin07.pdf](http://www.nhpf.org/library/site-visits/SV_Wisconsin07.pdf)

<sup>20</sup> Continuing education courses offered to nurses can be accessed at:

<http://mynursingce.son.wisc.edu/index.pl?id=20101>; online training courses must be taken and passed before social workers or nurses are certified to administer the screens; courses can be accessed at:

[http://dhs.wi.gov/lcaredatawarehouse/documents/LTCDW\\_User\\_Guide\\_v\\_1\\_2.pdf](http://dhs.wi.gov/lcaredatawarehouse/documents/LTCDW_User_Guide_v_1_2.pdf)

<sup>21</sup> Email dated 03/05/2010 from Karl Schlenker (SAMS Administrator) to all SAMS and Beacon users in Wisconsin indicating that Harmony's Beacon I&A database would be migrated into Wisconsin's statewide SAMS database over the weekend of March 5 through March 7 (2010).

---

<sup>22</sup> HSRS Mental Health Module – Section 12 contains five fields that are the multi-axial fields described in the *Diagnostic and Statistical Manual of Mental Disorders (DSM)*. The HSRS Mental Health Module can be accessed at: <http://dhs.wisconsin.gov/forms1/f2/f20855.doc>.

<sup>23</sup> Page 1 of the ForwardHealth Outpatient Assessment Form contains the five multi-axial fields in Section 2. The complete form can be accessed at: <http://dhs.wisconsin.gov/forms/F1/F11103.pdf>

<sup>24</sup> Form F-1103A containing completion instructions for *Outpatient Mental Health Assessment and Treatment / Recovery Plan*

<sup>25</sup> HIT Policy Committee Transcript; August 14, 2009; pages 1, 72 and 73. Dr. Peel's comments are on pages 72 and 73.

<sup>26</sup> HIT Standards Committee Meeting Transcript; May 15, 2009; pages 1 and 40; my comments are on page 40

<sup>27</sup> Copy of my email dated 05/15/2009 to the Office of the National Coordinator (ONC) offering to be a "volunteer use case"

<sup>28</sup> Copy of letter from Governor Doyle to Secretary Michael Morgan (dated April 15, 2008) releasing Metavante's privacy assessment of the State of Wisconsin's information systems. The complete report can be found on my website at: <http://www.metasteward.net/MetavantePrivacyAssessment041408.pdf>

<sup>29</sup> Cover, pages 1-4 and Appendix F of the Family Care Infrastructure Request for Information (RFI). The complete document can be viewed at: <http://dhs.wi.gov/lc/PDFs/RFI-1682.pdf>

<sup>30</sup> Email from Steve Harvancik project manager of the long-term support infrastructure project answering my question concerning BADR and also noting that Harmony was interested in the request for information (RFI) process.

<sup>31</sup> Copy of email to Steve Harvancik project manager informing him of the opportunity to comment on the Consumer Preferences Draft Requirements Document.

<sup>32</sup> Email from SAMS administrator advising me that any/all security issues had been addressed and that future security enhancements would be implemented