



6112 Exchange Street
McFarland, WI 53558
June 30, 2008

Rea Holmes, Executive Assistant
Department of Health and Family Services
1 West Wilson Street
Madison, WI 53707-7850

Tonya Harmon, CEO
Harmony, Inc.
12120 Sunset Hills Road
Reston, VA 20190

Re: Social Assistance Management System (SAMS): Secret Database that Breaches The
Fourth Amendment Privacy Rights of Elderly and Disabled Citizens

Dear Executives:

This letter is in response to messages (dated May 7, 2008) which I received from the State of Wisconsin (Rea Holmes) and Harmony's CEO (Tonya Harmon). These messages related to my observations that I presented to them (made as the Data Entry Volunteer for McFarland's Senior Outreach Program) concerning the Social Assistance Management System (SAMS). The letter and email that I received indicated that neither the Department of Health and Family Services (DHFS) nor Harmony, Inc. understands my concerns and the profound seriousness of the situation that now confronts the State of Wisconsin, Harmony, Inc. and the Administration on Aging (AoA).

In particular, I would like to address two of Tonya Harmon's statements in her email to me dated May 7, 2008. (*Please see Attachment 2 – pages 3-4*)

First, since it is factual that DHFS has annually contracted for the SAMS system since 2001, (which was two years before Windows 2003 was available), and that Harmony, Inc., according to press releases was founded in 1998, Tonya Harmon's assertion that Agingnetwork.com has run on Windows 2003 "*since its inception*" (as quoted below) simply can not be true.

“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.”

Because SAMS is running on Windows 2003, it also is factual that the security breaches documented in *Attachment 1 – pages 6-12* are not due to flaws in the system, as I had originally thought. Because Windows 2003 servers default to a lockdown status, remote desktop control, as shown in the screen shots, has to be enabled explicitly by someone (an insider at Harmony, Inc.) with administrative authority. As a “least privileged” user, I should not have been able to go outside the McFarland domain. The screen shots on pages 6-12 in Attachment 1 are *prima facie* evidence that SAMS has a serious security vulnerability relating to remote desktop control, which in Windows 2003, can only be explicitly enabled by a corporate insider. I have read that Forrester Research estimates that nearly 80 percent of all database attacks are internal and that Gartner Research estimates that more than 95 percent of intrusions that result in significant financial loss are perpetrated by insiders. Forrester and Gartner are leaders among independent technology and market research companies.

Next, I will address Tonya Harmon’s threat to me in her email dated May 7, 2008, when she wrote,

“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.”

Ms. Harmon, it is now up to you to explain your statements. My violating confidentiality obligations and any statements I’ve made about Harmony, Inc. (all factual) are not an issue.

It is out of place for a CEO of a vendor company to issue cautions, about public disclosure of information, to a private citizen (me) who first heard of Harmony’s SAMS system in August 2007, well after I had left employment with the State of Wisconsin. But, in this day and age, it’s not unusual for a corporation to change the subject and shift the focus of concern, from the actual victim (me), whose privacy has been breached, to the corporation itself, as potentially being the injured party. It is reasonable to assume that Harmony likely has successfully used threats as a tactic that has stifled other victims from exercising their constitutional rights of freedom of speech and the associated constitutional right of freedom of the press.

But, be that as it may, Tonya Harmon’s threat of a corporate challenge to me clearly implies that both the State of Wisconsin and her corporation, Harmony, Inc. believe their confidentiality rights override my Fourth Amendment rights to privacy. Because of their power to control funding and their financial and legal resources, the State and Harmony find the tactic of shifting blame to the victim very effective in silencing criticism, by intimidation. In Wisconsin, fear of retribution (lowering funding) by the State, has silenced most criticism by local staff and nutrition program participants, of DHFS’ administration of the nutrition program.

Because my experience as a social worker began in 1963, I have vivid memories of the old social welfare system. I recall progress in attempting to meet more of the needs of older Americans with passage of the Older Americans Act. Payment for medical care was nearly non-existent under the old programs of Aid to the Blind, Aid to the Disabled, Old Age Assistance, Aid to Dependent Children and the catch all, General Relief program. I remember reviewing medical payments under the Kerr-Mills Bill, the forerunner of Medicaid and Medicare which then were established in 1965.

In the 1970's, as a Social Services Planning Specialist, I recall establishment of the congregate and home delivered meals programs (in 1973). Federal privacy legislation was passed in 1974 in response to computerized matching of records. In 1977, the U.S. Privacy Protection Study Commission cautioned against the gradual erosion of individual liberties "...through the automation, integration and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."

Just because these laws were enacted in the 1960's and 1970's doesn't make them any less important today than they were then. Privacy legislation and the review of how computerized tracking systems (both governmental and private) can affect our Constitutional freedoms should be part of in-service training for all DHFS staff, both civil service and contract employees.

Harmony, Inc. and the State of Wisconsin have used the Social Assistance Management System (SAMS), which appears to be both benevolent and wholly justifiable, to egregiously violate the privacy laws. But as did Harmony's CEO, DHFS Privacy Officer, Kathy Johnson shifts the concern from the victim to concern for BADR staff by writing,

" 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."

While staff in BADR might have been respectful and conscientious, they have not administered the Older Americans Act programs in accordance with state and federal privacy laws. Furthermore, the SAMS administrator, Karl Schlenker, maintained two personal web domains named "dhfsbadr.org" and "dhfsbadr.com" which appeared to me, and I'm sure to others, as official DHFS web sites. But they were NOT official DHFS web sites, they were Karl Schlenker's private web sites.

Instructions and other informational materials for implementation of the SAMS program, as well as documentation of administrative activities that were not sanctioned within state law, were placed on Mr. Schlenker's private web sites. While I still have copies of some of these materials, the web sites have now been shut down, and evidence (conveniently for the State) from those sites is no longer available, for scrutiny as public records. The content of the web

sites, that were shut down by the State, should be identified as public records and be made available under Wisconsin's Open Records Law.

Speaking for Metasteward LLC, all my statements concerning Harmony's software are factual and are based on my personal observations of the SAMS system and information directly received from the State of Wisconsin as open records or other information publicly available on the Internet. Additionally, as a registered vendor with the State of Wisconsin, Metasteward LLC is considering challenging the procurement procedure that DHFS followed when it awarded Harmony, Inc. the contract for the SAMS tracking database in March 2008.

Although, in my open records request dated April 21, 2008, I characterized the SAMS system and Harmony's data centers as only having "suspected security vulnerabilities", documents, that I received as a result of my request, along with subsequent analyses of my observations and publicly available information, confirm that:

1. The Department of Health and Family Services (DHFS) has utilized the Social Assistance Management System (SAMS) to unlawfully and systematically breach the privacy of its elderly and disabled citizens by covertly constructing electronic records containing their protected health information (E PHI) since 2001.
2. The Social Assistance Management System (SAMS), as implemented by the Department of Health and Family Services, lacks the necessary security safeguards to protect the confidential information of elderly and disabled citizens who participate in the congregate meal and home delivered meals programs and their caregivers.
3. The entire population of participants in the Aging Network, through the proprietary AgingNetwork.com web site, has been vulnerable to cyber crimes of "identity theft" and "phishing" since Wisconsin implemented SAMS in 2001.

Before you (Harmony, Inc. and DHFS) again dismiss my concerns out of hand and deny the validity of my observations, please personally examine (at least look at) the screen shots included in the attached copies of:

- "1-ScreenShotsRemoteAccess.pdf"
- "2-HolmesHarmonEtcEmails.pdf"
- "3-FairfaxCountyAudit2006.pdf"
- "4- OpenRecordsRequest.pdf"

Compare your statements (in The Capital Times newspaper article, dated April 25, 2008, and those in your letters and emails) to my comments and the documented facts. It seems difficult for Tonya Harmon to comprehend that she herself was mistaken when she said of me, "*The gentleman is mistaken in what he thought he could have seen or done.*" Screen shots in the attached documentation will enable one to see that the entire National Aging Services Network, and all programs administered by the Administration on Aging, have likely been compromised on a nation-wide basis. If staff from DHFS and Harmony, Inc. had shown you

(Rea Holmes and Tonya Harmon) my documentation, you would have seen what I saw and realized what could have been done with the files. The screens shots below are ones that I gave to DHFS staff on at least four separate occasions but never received more than cursory denials that the SAMS system was vulnerable. I believe that attached documentation, if viewed objectively, will lead to the realization that my observations are accurate and represent the truth.

1-ScreenShotsRemoteAccess.pdf-

- Log on screenpage 1
- Screens from my personal electronic recordpages 2-5
- Screen showing Agingnetwork Citrix servers and Ctx02 highlighted pages 6-7
- Screen showing directories of (opened) Ctx02 server.....page 8
- Screens showing (a few) SQL tables of expanded directory SQL03TBLS...pages 9-10
- Screen showing host system documentation files.....page 11
- Screen showing host system files for Omnia Interviewerpage 12
- The Capital Times newspaper article dated April 25, 2008 – discrediting my observations.....page 13

Examination of pages 1-5 of the screen shots confirms my concerns relating to privacy. Anyone who looks at the database fields of my SAMS record, should be able to understand my concern and recognize that my privacy and the privacy of others was being violated. By establishing and specifying the responsibilities of its Public Records Board, Wisconsin has the strongest law among the states relating to publicly identifying record series containing personally identifiable information. DHFS has not followed state statutes in registering SAMS as a record series that contains personally identifiable information.

Selected sections of *Records Management Fact Sheet 9: Record Series Containing Personally Identifiable Information (revised January 2008)* follow:

“State statute 16.61 (3) (u) requires the Public Records Board to prepare a registry of state agency record series that contain personally identifiable information (PI).”

“The motivation of this law is to raise the general awareness of the potential threat to individuals’ personal privacy by government record-keeping activities. In particular, records in electronic/magnetic formats are easy to share and distribute which make the risk of invasion of privacy greater. The central premise is that if agencies identify record series containing PI information it would serve two purposes. First, agencies would become more sensitive to privacy related concerns. Second the requirement that PI information be identified and made available for public access provides a mechanism for citizens and the public to gain knowledge and awareness about the personally identifiable information that state government collects and maintains.

Examination of pages 9-10 of the screen shots confirms the vulnerability of SQL database tables relating to Older Americans Act programs in several states. Among the files are California files identified with acronyms. These likely signify California programs including:

CAC – California Aids Clearing House
DIHS – Division of Immigration Health Services
EOC – Emergency Operations Center
FSA - Farm Security Administration
IHSS - In Home Supportive Services
LFADCRC – Alzheimers Day Care Resource Centers
LFLINKAGES - Linkages Projects
SNP – School Nutrition Program
VNHC – Visiting Nurse and Hospice Care

While I did not open the files, I have no doubt that a cyber thief could copy not only these files but all files on the web site. I specifically mention the California files because California has the strongest law that serves as a model for other states concerning disclosures of data security breaches.

Wikipedia explains the notification portion of *California SB 1386* as follows:

“The statute requires notification if you meet the following: (1) Any agency that owns or licenses computerized data that includes personal information (2) shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data (3) to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

Cyber thieves have sophisticated equipment and many technological resources at their disposal. The screen shots (which are pictures of screens on the host server) clearly show that a “cyber thief” not only could access and copy all the files in the AgingNetwork.com, but because this is a web network, could follow the connections back to the user’s computers and compromise those as well.

A recent California case concerned the prosecution of a man who was known as a member of the “botnet underground”. During the court hearing, the defendant admitted that he gained access without authorization to hundreds of thousands of computers in the United States and that he remotely controlled these compromised machines through computer servers. Once in control of the “zombie” computers, the defendant used his “botnets” to search for vulnerabilities in other computers, intercept electronic communications and engage in identity theft.

Because of the high profile of AgingNetwork.com and the immense financial gain that could be brought by marketing confidential health data on the black market, it is reasonable to believe that the network has been compromised and that Harmony, Inc. under California law should notify California residents that their personal information is reasonably believed to have been acquired by an unauthorized person/persons.

The Capital Times newspaper article dated 4/25/08, includes the following reactions (to my open records request letter dated 4/21/08) from Harmony, Inc, and DHFS representatives :

Tonya Harmon, CEO of Virginia-based Harmony Information Systems, said the system has never been breached. She said Buhr is mistaken if he thinks the information was vulnerable. "The state and I both agree that there has been no security breach," she said. "No client data has been exposed at all. The gentleman is mistaken in what he thought he could have seen or done." (These comments are empty assertions without proof. There is no evidence that Tonya Harmon had even looked at copies of the computer screens that I had provided DHFS on many occasions.)

DHFS Executive Assistant Rea Holmes said even though Buhr could see the icons, he did not have the proper access to open or move them. The company has since changed the program so even the icons aren't visible, she said. "We take this very seriously," Holmes said. "Whenever there is a potential risk we make sure we work with the company right away. In this case there was never a data breach." (This is another example of statements made without substantiation. If Rea Holmes had looked at the screen shots, she would have seen that the files could have been opened. My point was, and still is, that without proper authorization I could have opened or deleted the files. Of course, I know that I didn't have the proper authority to open or move them, that was my main point concerning SAMS security. But even more importantly, the screen shots show, beyond a reasonable doubt that "cyber thieves" with their sophisticated high powered equipment can easily compromise the whole "AgingNetwork.com" web site.)

Karl Schlenker, who oversees the Harmony database for DHFS wrote, in an email to me, that he had stood up at a users conference to "*loudly declare that a significant security hole existed and must be immediately addressed.*" In the newspaper article, Diane Welsh, DHFS Chief Legal Counsel is quoted as saying, "*That significant security hole Schlenker described involved concerns over remote access to the site, which was quickly fixed by Harmony.*" (All my concerns were about remote access to the Harmony web site and security vulnerabilities that had existed prior to Harmony fixing them. Shouldn't Harmony have let nutrition program participants know that there had been a potential security problem? Were there other security lapses about which Harmony, Inc. did not inform DHFS? Do security vulnerabilities still exist today?)

Although my major concern related to privacy issues, Harmony and DHFS didn't even mention the privacy issues I was raising and instead focused on statements made by Karl Schlenker, a BADR contract employee who had said that he had stood up at a conference to "*loudly declare that a significant security hole existed and must be immediately addressed. That particular hole was fixed within the same week.*" Then with typical careful parsing of words, representatives of Harmony and DHFS proceeded to agree among themselves that there had been no security breach and that no client data had been exposed, in spite of the fact that it

was their own contract employee, Karl Schlenker , who had confirmed the security problem, rather than me.

The reactions by Harmony and the State indicate that they are in a state of denial and don't understand modern cyber threats and attacks. In the past, people hacked into networks to "prove that they could." While those attacks were malicious, recent attacks have been motivated by the quest for financial gain by the hacker. Attackers are seeking data to sell and are using advanced technology to identify vulnerable web sites. All access to SAMS, from state and local sites, is remote. All screen shots are of directories pictured through remote access to Harmony's host servers. While I chose not to open SQL tables containing client data, there is no reasonable doubt that those tables were remotely accessible. Likewise, while I chose not to run Omnia Interviewer executable files shown on page 12, there is no reasonable doubt that those files could have been remotely executed.

2-HolmesHarmonLetters.pdf – This file contains the following items:

- 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

After Rea Holmes of the Department of Health and Family Services (DHFS) and Tonya Harmon of Harmony, Inc. discredited my observations in the press, I received a letter and emails that further demeaned me. The threats by Tonya Harmon to my constitutional right of freedom of speech and the related right of freedom of the press are reprehensible. It is troublesome that the CEO of Harmony, Inc., a vendor company, under contract to the Department of Health and Family Services (DHFS), would issue threats to a private citizen in a personal email.

Even more troublesome is the fact that DHFS would participate in the cover-up both with their public statements and the internal directive from their Privacy Officer, Kathy Johnson, who wrote, *“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.”*

The simple fact of the matter is that my observations and assertions are true and it is a fact that the Department of Health and Family Services (DHFS) has been illegally collecting protected health information from seniors since signing the first SAMS contract in 2001. The public should be alarmed as the security deficiencies in the SAMS system are monumental and are the same deficiencies of the Harmony system that were pointed out in the report issued by the Fairfax County (Virginia) Internal Audit Office in September 2006. Kathy Johnson interprets my advocacy for senior citizens as an action that *“can only serve to falsely alarm senior citizens and should be vigorously denied.”* As the HIPAA Privacy Officer, Kathy Johnson should be at the forefront of advocating for the Fourth Amendment rights of the elderly and

disabled rather than directing DHFS staff to vigorously deny my advocacy efforts on behalf of senior citizens.

3-FairfaxCountyAudit2006.pdf –

This file is a copy of an audit report dated September 2006, of the Harmony system which was implemented by Fairfax County (Virginia) Human Services to replace an old mainframe system. The audit was conducted by the Fairfax County Internal Audit Office which was outside the staff or line management function of the Department of Human Services and free of organizational impairments to independence.

The “Executive Summary” in that report summarizes the findings as follows:

“Our audit found that access to the Harmony system did not incorporate proper separation of duties and the “least privilege” concept which is required by the county’s Information Technology Security Policy PM 70-05. Access request forms were not maintained and shared user accounts were allowed. Moreover, data in the system were modified without documented authorizations. Even though Harmony provides various reports and audit logs of user activities and system events, management review and monitoring were not performed. The above conditions have contributed to the following areas of weakness:”

- *“Opportunity for users to make unauthorized changes to critical application data”*
- *“Violation of the county’s Information Technology Security Policy”*

Other findings were:

- *“Vendor Addresses and their service price rates were changed in the vendor file without documented authorization.”*
- *“Access request and approval forms were not maintained for the twenty-two users that we tested.”*
- *“Seventeen of the twenty-five user profiles that we tested had access levels that prevented separation of duties.”*
- *“We found a total of forty-three shared user accounts where users were able to perform various tasks including update. PM 70-05 requires that all accounts be uniquely identifiable using the assigned user name.”*

Although the Harmony system audited is not the same as the SAMS system, the deficiencies noted are very similar to those that I observed in SAMS and documented in the table below:

Harmony System Audit – September 2006 - by Fairfax County Internal Audit Office	McFarland Senior Outreach Observations – 2008 – by Fred Buhr
<p>1. Access Controls and Separation of Duties</p> <p><i>“User account permissions were granted that would allow for a single user to add new vendors, process invoices and prepare checks for payment. Seventeen of the twenty-five use profiles that we tested had access levels that prevented separation of duties. Proper separation of duties dictates that tasks and associated privileges for a specific business process be disseminated among multiple users. The likelihood of fraud and errors are increased without proper separation of duties with the user account management process.”</i></p>	<p>1. Access Controls and Separation of Duties</p> <p>McFarland has only one account and login which is assigned to the Director of McFarland’s Senior Outreach Program. All business and data entry processes are conducted through this one account and login. Harmony’s SAMS system does not encourage proper separation of duties which dictates that tasks and associated privileges for a specific business process be disseminated among multiple users.</p>
<p>2. Access Request and Approval Forms</p> <p><i>“Access request and approval forms were not maintained for the sample of twenty-two users that we tested. In fact, access request and approval forms for all users from the time of the implementation of the Harmony system had been lost according to the Harmony system administrator. PM 70-05 state that every user account should have an associated request and approval for the level of access granted. Among other information, these forms should document management’s explanation as to the appropriateness of the access level being requested for the users. Management approval of the level of user access granted cannot be verified</i></p>	<p>2. Access Request and Approval Forms</p> <p>McFarland has only one login that is assigned to the Director of McFarland Senior Outreach Services and no access requests and approval forms have been completed for other users of the system. Because there is only one login for McFarland, it was an outright lie when the DHFS Privacy Officer said that, “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.” The password that was changed belonged to the Director of the McFarland Senior Outreach Program and she was only informed that her password had been changed after the fact. What the Privacy Office calls a “good</p>

<p><i>without documented access request forms.”</i></p>	<p>security practice” instead points out the extent that DHFS is willing to go in order to cover-up the lack of due diligence in protecting the confidential information of seniors that the Department collected in violation of State and Federal Privacy laws.</p>
<p>3. Account Management – Shared Accounts</p> <p><i>“We found a total of forty-three shared user accounts where users were able to perform various tasks including update. PM 70-05 requires that all accounts be uniquely identifiable using the assigned user name. This provides accountability by associating tasks performed with the user name that performed it. By allowing user accounts to be shared by two or more users, tasks performed could not be associated to the individual users thereby preventing accountability.”</i></p>	<p>3. Account Management – Shared Accounts</p> <p>In addition to the problems presented by shared accounts in being able to identify and place responsibility with individual users for changes to records, Wisconsin’s implementation of the Harmony system further complicates the matter by having shared accounts and passwords at the County and State levels so that it is virtually impossible to know who actually accesses and changes any senior’s electronic record.</p> <p>While Harmony and the State contend and forcefully deny any breach of privacy or security, I know for a fact that my record was changed after I had presented copies of it along with other system screen shots at my meeting with the Janie Riebe of Dane County and Amy Ramsey of DHFS on April 7, 2008. Contrary to the DHFS Privacy Officer’s assertion that I had resigned my volunteer duties, I had only suspended my data entry activities. In my letter to DHFS dated April 21, 2008, I said, “This is a follow up to my request of January 31, 2008, to Bureau of Aging and Disability Resources (BADR) staff asking that they cite the authority for the practice. Pending a response to that request, I am suspending my entering data into the SAMS tracking system.”</p> <p>On April 30, 2008, prior to receiving a response I sent an email to the Director of McFarland Senior Outreach and Dane County, saying, “I think that I’ve drawn enough attention to my request, for the</p>

	<p>State to respond to my question regarding their authority to mandate the Checklist, that I can comfortably end my suspension of entering data. Effective tomorrow, May 1st, I plan to resume the duties of my volunteer data entry job so McFarland doesn't fall behind. I'll drop by the Village Hall and pick up my password sometime tomorrow."</p> <p>The Director did, in fact, provide me with her proxy to again enter data and on May 5, 2008, I opened SAMS and looked at my own electronic record. I found that one field that I had filled had reverted back to a default setting indicating that someone had looked at my record and breached my privacy rights. I found that as a matter of conscience I could no longer enter data and told the Director that I could not participate as a data entry operator for the SAMS system until the nutrition data is moved to the Human Services Resource System (HSRS) and safely housed in Wisconsin's Data Center on Femrite Drive in Madison.</p>
<p>4. Changes to the Vendor File Not Documented</p> <p><i>“Vendor addresses and their service price rates were changed in the vendor file without documented authorization. Internal control procedures of DAHS Finance require authorization by the area manager or a designated staff before the vendor file can be modified. None of the twenty-two records tested had such authorization. Without the authorization form that shows the signature, date and the reason for the vendor file changes, unauthorized changes to the vendor file might go unnoticed.”</i></p>	<p>4. Changes to Files Not Documented</p> <p>Wisconsin’s implementation of SAMS has no discernable internal control procedures to document authorizations.</p>

<p>5. Review of Management Trail and Monitoring of System Activities</p> <p><i>There was no management review process to monitor the activities of the system administrator and special users (i.e. users who can approve invoices, and prepare checks). Currently, there are two system administrator and seven special users. These users had unlimited access to incompatible functions that hinder proper separation of duties. Unauthorized or erroneous changes to vendor information (i.e. vendor address change thereby sending payment checks to such address) can go unnoticed with a management review process.</i></p>	<p>6. Management Trail and Monitoring of System Activities</p> <p>No management review process is apparent in the Wisconsin SAMS system. Because of shared passwords and failure to follow any semblance of a “least privilege” security approach, unauthorized changes can occur at any point or any place in the system. There doesn’t appear to be even a semblance of a management process in place.</p> <p>If the Department of Health and Family Services would conduct a cursory internal audit of the SAMS system, the Department would find that the system does not meet either past or present information technology standards.</p> <p>There is no DHFS professional IT administrative oversight of the SAMS system. The result is that DHFS IT security policies are neither recognized nor followed.</p>
<p>6. Data Center Disaster Recovery Audit Report</p> <p><i>It was noted in a disaster recovery report that the Harmony system was at risk. The auditors noted, “ However, losing the capability to process, retrieve, and protect information maintained electronically, regardless of however it resides, can significantly affect a department’s ability to accomplish its mission. Examples of application at risk are: the Harmony System used for case and financial management in Family Services ... ”</i></p>	<p>6. Disaster Recovery</p> <p>The SAMS system data center often experiences outages in services. I have attached examples that include outages due to:</p> <ul style="list-style-type: none"> • Air conditioning failure – On October 3, 2007, the problem was described as follows: “There are two air conditioner condenser units in the AgingNetwork .com server room. One unit iced over. The second unit attempted to compensate, overloaded and failed. ... Our investigation of the impact of this event on AgingNetwork. Com found that 15 servers had shut down to prevent overheating.” • On January 29, 2008, Wisconsin’s SAMS system administrator sent an email to all AgingNetwork.com users

	<p>saying, “Synergy/Harmony experienced a network outage this morning between 9:15 and 9:50 AM CST. .. On a separate note, some of you may have experienced problems yesterday (Monday) afternoon while attempting to use SAMS and/or Beacon via AgingNetwork.com. When I noticed these problems mid-afternoon, I personally traced them to one of the internet’s primary data carriers (the company named “Level 3”). So.. Monday’s problem was not the fault of your/my internet” service provider(s) , nor was it the fault of Synergy/Harmony. Rather, it could be said that part of the internet itself was temporarily “broken”. .. Sorry for the inconvenience. I guess sometimes that’s just technology..”</p>
--	--

The report noted that the audit did not include a review of the general controls environment, including the security and controls over the SQL Server database in which the Harmony application data is stored. The auditors said that the effect of the scope limitation would be that if weaknesses existed in the general controls environment, it could have a negative impact on the integrity of the application data. My analysis has pointed out the vulnerabilities of the SQL Server database in SAMS. Through remote access to the root of Harmony’s web server I was able to identify the names of over 440 SQL Server tables in one directory alone. Screen shots of the first 30 along with the last 30 of the files in that directory are proof that those files were, and perhaps still are, vulnerable to criminal attacks.

4- OpenRecordsRequest.pdf –

This file contains the following:

- Copy of my open records request dated April 21, 2008.....page 1
- Copy of the contract for the SAMS system, first dated June 4, 2001pages 2-4
- Copy of the mandate and instructions dated January 29, 2008, issued by Amy Ramsey, Nutrition Specialist, Bureau of Aging and Disability Resources (BADR)...pages 5-6
- SAMS Docs – Nutrition Check Committee, Form and SAMS Data Entry..pages7-19
- “dhfsbadr.org” and “dhfsbadr.com” messages as of May 9, 2008page 20
- Documentation of SAMS Programs removed from dhfsbadr web sites.....pages 21-22
- Copy of my email to Rea Holmes dated May 15, 2008 – to which no reply has been received..... ..pages 23-26

On January 29, 2008, Amy Ramsey, the State of Wisconsin's Nutrition/Prevention Specialist, sent an email to all nutrition programs, saying, "Beginning 3/1/08 all nutrition programs will be required to use SAMS to track client nutrition data from the new Nutrition Screening Form that everyone was required to implement by 1/1/08." The email went on to say that SAMS entry and reporting instructions could be found at:

<http://dhfsbadr.org/docs/sams/nutritioncheck/>.

The Nutrition Specialist also said, "This data will be very useful to our nutrition programs because it will allow those at the local level to show nutrition outcomes and it will allow me to show nutrition outcomes at the state level."

Although it later would be disclosed that the "dhfsbadr.org" web site was privately owned by the SAMS database administrator, Karl Schlenker, at the time of the initial mandate, the site appeared to me to be an official site of the Department of Health and Family Services (DHFS) and that the instructions represented official State policy. Kathy Johnson, DHFS Privacy Officer, in her email dated May 2, 2008, to Mike Lettman, DOA Director of Information Security, said, "*As a convenience to SAMS users, Karl set up an Internet site where he deposited memos and materials to frequently asked questions... The site was established without following protocol for DHFS web postings... All material posted as policy was approved by management within the Division of Long Term Care/Bureau of Aging and Disability Resources.*" Protocol **should have been followed** and if protocol had been followed and the level of approval for establishing policy had been set at senior management levels in either the Division of Long Term Care or the Department of Health and Social Services, as it should have been, it is unlikely that BADR would have turned into a "rogue" unit that continually has flaunted state and federal privacy laws.

Kathy Johnson's statements in her email prompt many questions: How can a Privacy Officer cavalierly state that **protocol was not followed** for DHFS web postings but maintain that all material was approved by Division of Long Term Care management? Did the Division Administrator of Long Term Care know about the private web sites? Were the private web sites operated on DHFS computers or were they maintained on Karl Schlenker's own personal computers?

Being both a volunteer data entry operator and nutrition program participant, I completed the tracking form and entered the information into my own electronic record in SAMS. I immediately had a visceral reaction to my privacy being violated. On January 31, 2008, I sent an email to the Bureau of Aging and Disability Resources (BADR) staff. I requested that they cite the authority for mandating a surreptitious SAMS tracking system that would populate twenty-five fields of an electronic record that nutrition program participants knew nothing about. The paper assessment form used gave no indication that it was more than a self scoring stand-alone checklist to be discussed with a doctor or other qualified professional. My original concern was that my privacy and the privacy of other nutrition program participants was being systematically breached.

The questionnaire itself and the covert assessment process was an affront to the basic precepts of the Older Americans Act and social work practice in Wisconsin. After working as a public assistance case-worker (prior to Medicare and Medicaid) in Iowa, from 1963 to 1965, I was selected to participate as a social worker in a State of Wisconsin “educational leave program” in Milwaukee, Wisconsin.

My master’s thesis at the University of Wisconsin Milwaukee (UWM), co-authored with Robert J. VandeHei, was the development of an instrument that would, using a computer, quantify the relationships between elderly patient-family communication patterns and patients’ perception of isolation in nursing homes. Our study was one of many studies relating to legislation passed in 1965, including the Older Americans Act and the establishment of Medicare and Medicaid.

We developed an instrument that would yield the most useful and valid information when treated through computerized factor analysis. A patient’s perception of isolation was quantified using a semantic differential questionnaire while an assessment of interaction with a significant relative was measured using a standardized instrument to measure social interaction. At the time, there were only a few hundred mainframe computers in the country.

In 1970, after being a practicing counselor and social worker for nearly fifteen years, I accepted a position in the newly formed Division of Family Services (DFS) as a Social Services Planning Specialist. From 1970 to 1976 I staffed key division initiatives including development of the first Computer Reporting Network (CRN). I utilized techniques learned while at UWM to model social service case plans. Because of severe computer memory constraints, codes were used for items categorized into taxonomies. Current DHFS information systems such as the Human Services Reporting System (HSRS) are direct descendents of CRN. Included in the first information system, specified in 1973, were nutrition and congregate meals programs established under Titles VI and VII of the Social Security Act in that year.

Because both the mandate and approach being taken by the Bureau of Aging and Disability Resources are so out of line with social work practice standards and legal protocols of the Department of Health and Family Services, I thought that my questioning of the legal authority for the policy would prompt an immediate review and result in BADR rescinding the mandate. My only motivation was to reach a resolution to the issue and continue with my duties as a Data Entry Volunteer. Rather, my request for clarification has resulted in the denigration of me and six months of denials concerning my observations. As a matter of conscience, because my privacy was breached, and so as to not participate in continually invading the privacy of other participants, I had to leave my volunteer position. I had thoroughly enjoyed the duties of my position and I hope that these issues can soon be resolved.

As a former counselor and caseworker, with direct practice experience in mental health, developmental disabilities, and protective services, I was appalled at the implications of the illustration BADR used to show the correct way to code data entries and compare a participants’ initial assessment with a reassessment. In that illustration, a client’s health risk

was improved (dropping the client out of the high risk category) by eating more fruits and vegetables even though the client still consumed three or more drinks of beer, liquor or wine almost every day combined with six prescription drugs per day. Much lower alcohol consumption, as low as more than one drink per day for both elderly men and women, is identified as a cause for concern by alcohol/drug dependency professionals. Regularly consuming alcohol with prescription drugs is cause for concern in and of itself. *The Geriatrics Review Syllabus (GRS), 5th Edition 2002-2004, page 244* defines “heavy” drinking as a minimum of 12 to 21 drinks per week. The illustration used by BADR indicates the client consumes at least 21 drinks per week which is at the higher end of “heavy” drinking.

Furthermore, BADR does not appear to understand that success of the nutrition program is more accurately judged by the overall increase in numbers of elderly and disabled who can remain in their own homes as they become sicker or more disabled rather than the number of individuals whose nutritional risks are diminished as assumed by the mandated assessment checklist. The “new” use of the self scoring checklist “DETERMINE” as an assessment and reassessment tool to indicate an individual’s “progress” relative to specific risk factors, with scores entered into twenty five electronic fields, is totally out of keeping with the tool’s use as described in the *The Geriatrics Review Syllabus (GRS), 5th Edition 2002-2004, on page 194*. The checklist was developed in the late 1980’s and was created to raise public awareness of the importance of nutrition to the health of older persons. It is a self-reporting tool that is widely used and recognized as a private and confidential questionnaire.

The familiarity of the form, without any indication to the contrary, creates the expectation of privacy. On page 195 of *The GRS*, Table 28.5 identifies risk factors for poor nutritional status as:

- Alcohol or substance abuse
- Cognitive dysfunction
- Decreased exercise
- Depression, poor mental health
- Functional limitations
- Inadequate funds
- Limited education
- Limited mobility, transportation
- Medical problems, chronic diseases
- Medications
- Poor dentition
- Restricted diet, poor eating habits
- Social isolation

The risk factors as reflected in the “DETERMINE” tool are relevant to a context involving many more disciplines than that of nutritionists alone. By BADR focusing only on using the tool to assess nutritional risk and not consulting with mental health and other drug abuse professionals in DHFS and not even consulting with long term care specialists located in the same room at 1 West Wilson Street, their program has been developed with little sensitivity to

privacy issues and a lack of recognition that the risk factors are confidential personal health information covered under privacy laws.

It is clear that the “DETERMINE” screening tool was intended to be utilized by a patient with their physician or other health professional, not as a form to collect information for a person’s electronic health record. Instructions for a score of 6 or more read: *(Please see Attachment 4, page 8)*

“You are at high nutritional risk. Bring this checklist the next time you see your doctor, dietitian or other qualified health or social service professional. Talk with them about any problems you may have. Ask for help to improve your nutritional health.”

In looking at the form itself, there is no hint, in the least, that all entries are going to become a part of a person’s electronic record, and that the individual scores are going to be used by the State to evaluate the state wide nutrition program. If anything, instructions on the form enforce an expectation of privacy by anyone who completes the form. Using the form to collect information and then recording that information in personally identifiable electronic records in the SAMS database is an egregious violation of nutrition program participants’ Fourth Amendment rights to privacy.

I have structured this letter around a review of my observations and other publicly available information concerning Harmony’s software. In summary, this review can be compared to selected rules of best practice found in the HIPAA Security Series issued by the Centers for Medicare & Medicaid (CMS). Paper 6 of the Series adapted content developed by the National Institute of Standards and Technology (NIST) presented in its publication, *SP 800-30 – Risk Management Guide for Information Technology Systems*.

The Department of Health and Family Services (DHFS) and Harmony Inc. have failed to exercise due care and diligence in the implementation and operation of the SAMS system and should be held accountable. DHFS and Harmony, Inc. have failed to:

- “Implement policies and procedures to prevent, detect, contain, and correct security violations.”
- “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information.”
- “Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.”

Important definitions to understand include:

- Vulnerability – “A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or

intentionally exploited) and result in a security breach or a violation of the system's security policy.”

- Threat – “The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”
 - “Natural threats may include floods, earthquakes, tornadoes, and landslides.”
 - “Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.”
 - “Environmental threats may include power failures, pollution, chemical, and liquid leakage.”
- Risk – “The net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur... Risks arise from legal liability or mission loss due to:”
 - “Unauthorized (malicious or accidental) disclosure, modification, or destruction of information”
 - “Unintentional errors and omissions”
 - “IT disruption due to natural or man-made disasters”
 - “Failure to exercise due care and diligence in the implementation and operation of the IT system.”

Summary and Conclusions

Although I have spent considerable time and effort up to this point researching these issues, I have seen nothing that would indicate that either DHFS or Harmony, Inc. comprehends my concerns. My time spent researching and presenting the facts should be met with more than threats and accusations such as, “*The gentleman is mistaken in what he thought he could have seen or done.*” DHFS and Harmony have presented no proof to support assertions that the SAMS files haven't been vulnerable to malevolent cyber attacks. Furthermore, you (Rea Holmes and Tonya Harmon) have offered no proof that DHFS is even authorized by law to operate the SAMS system.

Pages 23-26 of Attachment 4 contain a copy of my email to Rea Holmes dated May 15, 2008. I have not received a reply to that email in which I explicitly identify the state and federal privacy laws that DHFS has violated since June 4, 2001, when DHFS first signed a contract for the SAMS system. My main concern was, and still is, the invasion of privacy of

participants in the nutrition programs. An electronic health record has been constructed for each nutrition program recipient.

Pages 2-5 of Attachment 1 are copies of a few of the screens from my personal record in SAMS. Wisconsin law views each of the screens as a form. Every data entry field is considered to be a form field. In aggregate, all of the potentially hundreds of data entry fields that can be filled with information, are considered as a personally identifiable electronic record.

My electronic record contains fields including, (but not limited to): SSN, Birth Date, First Name, Last Name, Marital Status, Gender, Medicaid #, Medicaid Policy #, Medicare #, Medical Assistance ID, Monthly Household Income, Monthly Individual Income and a complete range of fields relating to caretakers. There are hundreds of available fields for confidential information, utilization of which is totally at the discretion of Bureau of Aging and Disability Resources (BADR) staff. Program participants are not aware of the electronic records that are being maintained and statutorily required notices are not placed on the paper forms used to collect information from the participants. Nor are Wisconsin's laws met regarding registration of electronic personally identifiable records. Many of the fields in a person's electronic record are "linker fields" to that same person's record in another database. For instance, Medicare # is a key field to a person's record in another database as are SSN and Medical Assistance ID's. The SAMS database is the "linker database" to an unknown number of other databases.

Wisconsin statutes require state agencies to register such record series with the Wisconsin Public Records Board. The purpose of the law is to insure that state agencies do not maintain secret files on individual citizens. Because the Department of Health and Family Services has not registered the Social Assistance Management System (SAMS) with the Wisconsin Public Records Board, individuals are unable to access their own records in order to review, correct or update the personal information in those files. **The inescapable conclusion is that SAMS, under Wisconsin law, constitutes a system that maintains secret files on individual citizens in violation of their rights under the Fourth Amendment.**

Pages 8-9 of Attachment 1 are copies of screens showing approximately 60 SQL tables (out of over 440 that I saw in that directory) that are identified with acronyms representing Older Americans Act programs in various states. There should be no question in your minds that these files can be opened, copied, or deleted by anyone who can remotely access Harmony's servers at this level. **Because of the high profile of AgingNetwork.com and the immense financial gain that could be acquired through marketing the confidential information on the black market, it is reasonable to believe that the entire network has been compromised and that personally identifiable confidential information has been acquired by unauthorized persons and/or entities.**

Pages 11-12 of Attachment 1 are copies of screen prints showing access to "Program Files" on Harmony's web server. Again there should be no question in your minds that these files can be opened, copied, deleted or run on the web server. Since these files are at the "root" of

the server and because of the high profile of AgingNetwork.com and the millions of dollars that could be acquired by marketing the data on the black market, it is reasonable to believe that all Harmony's programs such as **Beacon, NorsReporter, OmbudsManager, Omnia Designer, Omnia Interviewer**, as well as SAMS have been compromised. Additionally, because connections to Harmony's web applications are two way channels of communication, it is reasonable to believe that all computers and the thousands of authorized users connected to Harmony's web server have been compromised. Also, because the SAMS system directly connects through the National Aging Program Information State Reporting Tool (NAPISSRT) module to the Agency on Aging (AoA) system, it is reasonable to believe that the nation-wide AoA system has been compromised.

As I mentioned earlier, cyber hacking has left the province of high school age children who would attack databases just to show it could be done and now is motivated by the quest for financial gain. Attackers are seeking to sell or otherwise maliciously use confidential data. They possess the advanced technology to identify vulnerable sites. AgingNetwork.com is a high profile site that, beyond a reasonable doubt, attracts cyber criminals intent on making financial gain through malevolent activities using confidential information of the elderly and their caretakers..

When I was a part of the group designing the Computer Reporting Network (CRN) in the early 1970's, which as I have noted, is the grandparent of the current Human Services Reporting System (HSRS), the motivation for developing systems was to show it could be done out of a sense of public service. I and the others of our original CRN group were all civil service employees. We conceptualized the system (brainchild of Tom Corbett) on a Saturday afternoon, in the summer of 1972, in Tom Corbett's living room, on our own time. (Tom Corbett has since published numerous scholarly articles on systems integration, over many years, at the Institute for Research on Poverty, University of Wisconsin.) Motivation for systems now has changed to one of a quest for financial gain by vendors. Original systems, referred to as legacy systems, have been replaced with outsourced vendor systems. Civil service employees have been replaced with contract employees. With the decline in numbers of civil service employees, institutional memory of the origins of legacy systems and landmark achievements, such as the 1970's privacy laws, is missing and public service is diminished.

In conclusion, I urge you to take my observations seriously. Although you can continue to deny and maintain the pretense that I don't know what I've seen or what I could have done with what I didn't see, the truth will eventually come out, and you will have to deal with accepting responsibility for the vulnerabilities of the SAMS system. Do not send me more replies that personally discredit me and denigrate my observations. Staffs at the Wisconsin Department of Health and Family Services and Harmony, Inc. have an obligation to respond in a professional, mature, and civil manner and should have a sincere desire to find a resolution to these very important issues.

Please consider that seniors, the disabled and all visitors are making an uninformed choice to forego their Fourth Amendment rights when they register for congregate or home delivered

Department of Health and Family Services (DHFS) and Harmony, Inc. have not followed state and federal privacy laws in implementing the SAMS system in Wisconsin. Visitors to McFarland's nutrition site include village officials as well as presenters of programs and others. All have been asked to complete registration forms and the "DETERMINE" checklist. The information then has been entered into their SAMS electronic records. All have had their privacy breached by virtue of the fact that their confidential information was entered into the Social Assistance Management System (SAMS) without their informed consent.

Sincerely,



Metasteward LLC
Fred Buhr, Registered Agent

Attachments:

"1-ScreenShotsRemoteAccess.pdf"

"2-HolmesHarmonLetters.pdf"

"3-FairfaxCountyAudit2006.pdf"

"4- OpenRecordsRequest.pdf"

Copies to:

Scott Bauer, Associated Press
Joe Vanden Plas, Wisconsin Technology Network
Barbara Quirk, Geriatric Nurse Practitioner
Valerie Cook, Administration on Aging