

¹ *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>

MODEL STANDARDS OF FAIR INFORMATION PRACTICES

To date, most data privacy guidelines developed in industrialized nations share a core set of principles that are applicable to state and local government as well as the private sector. These fundamental principles are summarized below.

Secrecy: No secret record-keeping systems containing personally identifiable information should be maintained, consolidated, centralized or cross-tabulated.

Transparency: Data processing and information handling activities should be transparent. Data subjects should be informed what information is being collected, how it will be used and with whom it will be shared.

Collection Limitation: Personal information should be gathered in a fair and lawful manner. Data collection should be limited to what is necessary for a specific purpose or task. Data collection that is not required or mandated should be labeled "voluntary."

Record Access & Accuracy: Individuals should be permitted to review their own personal information contained in records. They should also be allowed to copy and challenge the accuracy of that information and amend it, if appropriate.

Limitations on Secondary Uses: Personal information should not be disclosed or reused for purposes other than for which it was originally collected, unless specifically required by law. If information obtained for one reason is subsequently re-released, consolidated, cross-tabulated and/or interconnected for some secondary purpose, the data subject should be informed and provide consent.

Accountability: Policies and procedures should be developed and implemented that ensure data integrity and confidentiality to the extent permitted by law. A privacy officer who is accountable for compliance and privacy safeguards should be appointed. Annual employee training in ethical conduct and protection of sensitive data should be required.

Data Quality & Integrity: Personal data must be accurate, complete and up-to-date. There must be recognition of and accountability for errors that are perpetuated electronically.

Computer Security: Computer security safeguards that anticipate technological change and recognize the capabilities of new applications should be implemented. Such policies must also guard against factual alteration, destruction and unauthorized release of data.

² 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



State Aging Information Systems Management Study

Final Report

Prepared for the:

**National Association of State Units on Aging
1201 – 15th Street, NW
Suite 350
Washington, DC 20005**

Prepared by:

**Westat
1650 Research Blvd.
Rockville, MD 20850**

December 2006

Table 1a: SUA Information Management Systems that Support OAA Reporting

State	Initial Survey Results						Post-Survey				
	Inhouse/ Custom- developed	Commercial			Contract with a university	Manual or Excel	In-house/ Custom- developed	Commercial			
		AIM	SAMS	Other				AIM	NAPIS- Care (RTZ)	SAMS	Other
AL	✓					✓					
AR						✓		new			
AZ	✓						pre-rfp				
CA	✓						rfp				
CO			✓							✓	
CT	✓									new	
DC					✓					new	
DE	✓						pre-rfp				
FL	✓						✓				
GA	✓						✓				
HI			✓							✓	
IA	✓						✓				
ID			✓							✓	
IL				✓							✓
IN	✓						✓				
KS	✓						✓				
KY						✓				new	
LA			✓							✓	
MA	✓									new	
MD		✓						✓			
ME	✓									new	
MI	✓						✓				
MN		✓						✓			
MO	✓						✓				
MT	✓						✓				
NC	✓						✓				
ND			✓							✓	
NE	✓						✓				
NH	✓						✓				
NJ	✓									new	
NM			✓							✓	
NV	✓									new	
NY	✓						✓				
OH			✓							✓	
OK		✓						✓			
OR	✓						✓				
PA			✓							✓	
RI			✓							✓	
SC		✓						✓			
SD			✓							✓	
TN			✓							✓	
TX						✓				new	
UT	✓								new		
VA		✓						✓			
VT			✓							✓	
WA			✓							✓	
WI			✓							✓	
WV	✓						✓				
WY			✓							✓	
#	24	5	15	1	1	3	18	5	2	23	1

provider staff interviews. Perhaps most influential in Ohio's selection of SAMS was the Cleveland AAA's current use and endorsement of this software.

The SUA in South Carolina selected the Advanced Information Manager (AIM) developed by Saber Corporation. The SUA and AAAs considered several approaches, but AIM was already being used successfully by several AAAs in the state, which essentially explains South Carolina's selection of this product. The SUA and AAAs do not administer Medicaid Waiver programs, and these agencies use AIM for OAA client tracking and SPR reporting purposes. However, some of the same providers that deliver OAA services also operate Waiver programs under separate contracts with the state Medicaid agency, using a separate, state-mandated computer information system. Some of these providers use AIM to track clients under both programs and then export the Waiver data for entry (manually) into the state's Web-based Medicaid reporting system. However, a more functional integration of these two applications was of interest to these providers in order to eliminate redundancy.

Oregon developed a state-wide Medicaid software application, in house, which included the Waiver programs that the SUA and AAAs administered. The timing of this Oregon Medicaid MIS work coincided with AoA's SPR initiative and the corresponding efforts by the SUA and AAAs to address these reporting requirements. The SUA and AAAs asked the state to incorporate the OAA requirements within the Medicaid software, resulting in a single application that addressed the information needs of both programs. The 90/10 percent federal/non-federal funding from CMS for this software development was an important reason for integrating Medicaid and OAA computer applications, which other states may want to consider.

The fifth state we visited, Georgia, selected a software development consulting firm as part of an effort to build an enterprise-level application that would address the information needs of many state agencies, including the SUA. The economies of scale and benefits of coordination warranted such an approach, including the availability of state IT staff, who would maintain this system after the vendor completed the initial work. According to SUA staff, this enterprise-level application did not address all SUA requirements, and as a result the state IT staff then re-configured the vendor-developed system to meet the specific needs of the SUA, AAAs, and

HIPAA Compliance

Approximately 57 percent of the SUAs reported that their information systems are compliant with HIPAA confidentiality requirements. Given the uncertainty about what constitutes HIPAA compliance, the remaining states are not necessarily out of compliance. We found during the site visits that there was considerable confusion within the SUA and the state Medicaid agency, among others, about the specific requirements of HIPAA and any limitations this law imposes on sharing data among the SUA, AAAs, and service providers. This pertains directly to the information pooling objective of the NASUA study, which is designed to avoid the need for clients and caregivers to provide the same information more than once when registering for and receiving services.

Case Management

Under the case management heading, Table 5 also shows that 69 percent of the SUA information systems have a client assessment component, including documenting limitations in Activities and Instrumental Activities of Daily Living (ADLs and IADLs). As a related step in the case management process, care planning was a function supported by 53 percent of these information systems, including arranging for the services that clients need.

One interesting finding from the case studies was the presence of software utilities that use a range of client functional status and health data, in conjunction with demographic information, to construct composite measures of service needs. These computer applications use very detailed data about the client, including an in-depth profile of ADL and IADL limitations. For example, the two most frequently used commercial software products, SAMS and AIM, have algorithms that simulate the case management process and recommend an array of services based on certain underlying functional status, health, and demographic data from client registration and assessment instruments. In addition to the commercial vendor packages, the in-house information systems we reviewed during the site visits also include these assessment and service planning capabilities. For example, Georgia has what it calls the Determination of Need assessment instrument, which it revised from an original protocol, called the DON-R.

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

Agenda

❖ The Latest Headline

- April 5, 2008 – Audit: UW campuses must do more to protect data
 - “Defining data that need priority for protection and what level of protection is acceptable is basic to computer security - ”
 - “Corporate Sloppiness Is the Real Culprit for Data Loss, Not Vilified Hackers”
 - In the first quarter of 2007, electronic records – those containing Social Security or credit card numbers, academic grades or medical history – were bleeding out of North American organizations at the rate of 6 million a month – up some 200,000 a month from 2006.

❖ Harmony Information Systems, Inc.

- March 24, 2008 – News Release
 - Probably 200,000 Wisconsin records and millions of records nationwide from over 40 states
 - What kind of records? Review record format and point out that birth date and last four digits of SSN are case identifiers and appear on all screens and all case specific reports.
 - Recent IBM seminar – “Most security breaches occur internally”
 - “How much is personal data worth – Point out that the SAMS records are “Consumer records” and since they likely aren’t subject to HIPAA requirements, listings could be circulated for marketing purposes

❖ Chronology – Read excerpts

- September 25, 2007 to January 29, 2008 – System problems, especially note October 3
- January 29, 2008 – Mandate to use SAMS to track client nutrition data
- January 31, 2008 – Request to cite authority
- February 13, 2008 – Concerns about SAMS security
- February 18, 2008 – Plea to contact DHFS Security Officer
- February 20, 2008 – Phone call, computer problems and SB487
- March 3, 2008 – Assurance that concerns are taken seriously
- March 7, 2008 – Evaluation PPT and volunteer to help with statistics
- March 12, 2008 – Windows 2000 issues
- March 16, 2008 – “Nulls” security flaw screen shots
- March 18, 2008 – “Nulls” security flaw technical article
- Undated 2008 – Assorted system screen shots

❖ Conclusion - Discussion

- April 3, 2008 – Four pages
- Fair Information Practices – Confidentiality Agreement
- Whitepaper – Addressing the Insider Threat

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

SCAN-X-MESSAGE: NOTSPAM O:14 S:99 R:95 P:95 M:97 C:98
Return-Path: <CRAWFCH@dhfs.state.wi.us>
Date: Mon, 07 Apr 2008 14:04:19 -0500
From: "Charles Crawford" <CRAWFCH@dhfs.state.wi.us>
To: <fredbuhr@merr.com>
Cc: "Kathy Johnson" <JohnsKL@dhfs.state.wi.us>,
"Thomas Rapa" <RapaT@dhfs.state.wi.us>
Subject: Social Assistance Management System (SAMS)
Content-Disposition: inline
X-pstn-neptune: 0/0/0.00/0
X-pstn-levels: (S:14.47928/99.90000 CV:99.9000 R:95.9108 P:95.9108 M:97.0282
C:98.6951)

Fred,

Thank you for meeting with Tom and I on Monday, April 7th. The information you were kind enough to provide will spur two separate issues for our group.

1. The Citrix information will be given to our Citrix people here, to determine if this indicates a security issue to them.
2. We will take up the question of the use of the information by the company in question, to include:
 - Is there a confidentiality agreement in place with this company?
 - What requirements apply to inform users of the uses for the information gathered?

We will meet next week with Kathy Johnson, the DHFS Privacy Officer and the Privacy Officer for the Division of Long Term Care and present the information you gave to us. We don't know what can be done, but certainly the issues can be raised.

As a final note, it was gratifying to hear how responsive you felt the SAMS people located here have been.

Fred, thanks again.

Chuck Crawford, Deputy Continuity and Security Manager
Division of Enterprise Services
Wis. Dept. of Health and Family Services
PO Box 7850
1 W. Wilson St.
Madison, WI 53707-7850
Phone 608 266-8439
Fax 608 267-6749
E-mail crawfch@dhfs.state.wi.us

⁵ Article by Scott Bauer, Associated Press at: http://www.phiprivacy.net/documentation/2008/WiDHFS_02.html
accessed on 03/07/2010

Health-care company, state deny personal data was at risk

April 24, 2008

Scott Bauer

<http://www.madison.com/wsj/home/local/283134>

The security of a database containing sensitive information about 240,000 senior citizens and disabled people in Wisconsin was never breached or at risk, the chief executive of the company that controls the data said Thursday.

A top official with the state Department of Health and Family Services also sought to assure the state's senior citizens, saying their personal information was never in jeopardy.

The statements came in spite of an e-mail from a state official who said he had identified a "significant security hole" with the database and a comment from a senior center volunteer who said he had found a problem that could lead to thousands of records being compromised.

That volunteer, longtime state Department of Health and Family Services employee Fred Buhr, said he was able to see data files of people from around the country. Even though Buhr said he didn't open them, he believed they could have been viewed, altered or deleted.

There have been no known reports of the data, including Social Security numbers and addresses, being stolen or compromised.

Tonya Harmon, chief executive officer 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."

Buhr, who worked on data security for the state during his 41-year career before leaving in 2006 and starting his own data security company, disagreed with Harmon.

"I believe that I could have deleted a whole file," he said Thursday. "I believe that I shouldn't have been able to see the Texas files."

'Security hole'

Buhr was working as a volunteer entering data into the system from the McFarland senior center. The information on the database could have been viewed by 400 similar volunteers across the state and perhaps others who have access to the system across the country, he said.

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."

Karl Schlenker, who oversees the Harmony database for DHFS, said in a March 3 e-mail to Buhr that he had identified at least two problems with the system.

In the e-mail, Schlenker describes standing up at a conference attended by users of the software to "loudly declare that a significant security hole existed and must be immediately addressed. (That particular hole was fixed within the same week)."

He goes on to tell Buhr that he knew about the other problem that Buhr brought to him.

Schlenker said he was working with Harmony to "tighten down" the database "so that it is as secure as it can possibly be."

That "significant security hole" Schlenker described involved concerns over remote access to the site, which was quickly fixed by Harmony, said Diane Welsh, DHFS chief legal counsel.

Lawmakers angry

News of a possible security breach had Wisconsin lawmakers angry and seeking answers. There have been three cases since 2006 in which Social Security numbers were visible on state mailings.

State government has an "enormous problem" protecting private information and this latest case is "deeply troubling," said Sen. Ted Kanavas, R-Brookfield.

"These have been issues that have been public and widespread," he said. "I just don't get a sense that there's an emergency being applied to solving these."

State Rep. Marlin Schneider, D-Wisconsin Rapids, a longtime advocate of privacy rights, said the Legislature should have been informed about the concerns.

He serves on a recently created committee that oversees information policy and technology.

The committee has requested a briefing with DHFS officials to get more information, said the panel's co-chair, Rep. Phil Montgomery, R-Ashwaubenon.

Harmony's Social Assistance Management Systems program, used by Wisconsin since 2001, gathers nutrition, caregiver and transportation information about senior citizens and Meals on Wheels recipients to meet federal reporting requirements.

Harmony Information Systems says it is the industry leader in providing software and consulting services for the health and human services sector. Tommy Thompson, the former Wisconsin governor and U.S. Health and Human Services secretary, is a member of the company's board of directors.

⁶ 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>

Unofficial Text (See Printed Volume). Current through date and Register shown on Title Page.

Chapter Adm 12

ELECTRONIC RECORDS MANAGEMENT—STANDARDS AND REQUIREMENTS

Adm 12.01 Authority.
Adm 12.02 Purpose.
Adm 12.03 Scope.

Adm 12.04 Definitions.
Adm 12.05 Provisions.
Adm 12.06 Initial applicability.

Note: Chapter Adm 12 as it existed on November 30, 2000 was repealed and a new chapter Adm 12 was created effective May 1, 2001.

Adm 12.01 Authority. This chapter is promulgated under the authority of s. 16.611, Stats., state public records, s. 16.612, Stats., local government records, and s. 227.11 (2) (a), Stats., to implement s. 16.61, Stats.

History: Cr. Register, November, 2000, No. 539, eff. 5-1-01.

Adm 12.02 Purpose. The purpose of this chapter is to ensure that public records in electronic format are preserved and maintained and remain accessible for their designated retention period.

History: Cr. Register, November, 2000, No. 539, eff. 5-1-01.

Adm 12.03 Scope. This chapter establishes defined requirements, standards and guidelines for state and local government accessibility of electronic public records from creation through active use, long-term management, preservation and disposition. This chapter does not require an agency to maintain public records in electronic format.

History: Cr. Register, November, 2000, No. 539, eff. 5-1-01.

Adm 12.04 Definitions. In this chapter:

(1) "Accessible" means information arranged, identified, indexed or maintained in a manner that permits the custodian of the public record to locate and retrieve the information in a readable format within a reasonable time.

(2) "Accurate" means all information produced exhibits a high degree of legibility and readability and correctly reflects the original record when displayed on a retrieval device or reproduced on paper.

(3) "Authentic" means the retained electronic record correctly reflects the creator's input and can be substantiated.

(4) "Content" means the basic data or information carried in a record.

(5) "Context" means the relationship of the information to the business and technical environment in which it arises. "Context" can include, but is not limited to, such elements as: the origin of the record; date and time the record was created; identification of the record series to which the information belongs.

(6) "Electronic format" includes information created, generated, sent, communicated or stored in electrical, digital, magnetic, optical, electromagnetic or similar technological form.

(7) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data.

(8) "Legible" means the quality of the letters, numbers or symbols can be positively and quickly identified to the exclusion of all other letters, numbers or symbols when displayed on a retrieval device or retrieved by device or reproduced on paper.

(9) "Life cycle" means all phases of a record's existence: creation, active use, preservation and management through to disposition. "Disposition" includes permanent preservation as well as designation for destruction.

(10) "Meaning" means a record carries its original content, context and structure throughout its life cycle.

(11) "Public record" has the meaning given in s. 16.61 (2) (b), Stats.

(12) "Readable" means the quality of a group of letters, numbers or symbols is recognized as words, complete numbers or distinct symbols.

(13) "Reliable" means the electronic record produced correctly reflects the initial record each time the system is requested to produce that record.

(14) "Structure" means the appearance or arrangement of the information in the record. "Structure" can include, but is not limited to, such elements as heading, body and form.

History: Cr. Register, November, 2000, No. 539, eff. 5-1-01.

Adm 12.05 Provisions. State and local agencies shall comply with all statutes and rules relating to public records. With regard to public records stored exclusively in electronic format, state and local agencies shall do all of the following:

(1) Maintain electronic public records that are accessible, accurate, authentic, reliable, legible, and readable throughout the record life cycle.

(2) Document policies, assign responsibilities, and develop appropriate formal mechanisms for creating and maintaining electronic public records throughout the record life cycle.

(3) Maintain confidentiality or restricted access to records or records series maintained in electronic format, limiting access to those persons authorized by law, administrative rule or established agency policy.

(4) Utilize information systems that accurately reproduce the records they create and maintain.

(5) Describe and document public records created by information systems.

(6) Document authorization for the creation and modification of electronic public records and, where required, ensure that only authorized persons create or modify the records.

(7) Design and maintain new information systems so that these systems can provide an official record copy for those business functions accomplished by the system.

(8) Develop and maintain information systems that maintain accurate linkages, electronically or by other means, to transactions supporting the records created where these linkages are essential to the meaning of the record.

(9) Utilize information systems that produce records that continue to reflect their meaning throughout the record life cycle.

(10) Utilize information systems that can delete or purge electronic records created in accordance with the approved retention schedule.

(11) Utilize information systems that can export records that require retention to other systems without loss of meaning.

(12) Utilize information systems that can output record content, structure and context.

(13) Utilize information systems that allow records to be masked to exclude confidential or exempt information.

History: Cr. Register, November, 2000, No. 539, eff. 5-1-01.

Unofficial Text (See Printed Volume). Current through date and Register shown on Title Page.

Adm 12.06 Initial applicability. This rule first applies to public records stored exclusively in electronic format and to information systems acquired or substantially modified after the effective date of the rule.

History: Cr. Register, November, 2000, No. 539, eff. 5-1-01.

Records Retention / Disposition Authorization

<ul style="list-style-type: none"> Instructions for completion are provided on pages 2-3. In accordance with s.16.61, Wis. Stats, this form must be completed and approved by the Agency and the Public Records Board (PRB) within one year of creation of the records series and prior to disposition of any public record. Field #1 - Agency Records Officers generally assign sequential RDA numbers which are subject to PRB approval. If the agency does not assign an RDA number, leave this field blank and the PRB will assign the number. Agency Records Officer: Review & approve RDA; Assign RDA #, if applicable. Forward original <u>only</u> to the PRB. Maintain an agency copy during the Board's review process. 	<p>1. Retention/Disposition Authorization # (RDA)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Sequential Number</td> <td style="width: 50%;">Suffix Number</td> </tr> <tr> <td>2. Agency Number</td> <td>3. Unit Number</td> </tr> <tr> <td colspan="2"> 4. RDA Status <input type="checkbox"/> New <input type="checkbox"/> Amended <input type="checkbox"/> Sunset/Renewal <input type="checkbox"/> Closed/Superseded </td> </tr> </table>	Sequential Number	Suffix Number	2. Agency Number	3. Unit Number	4. RDA Status <input type="checkbox"/> New <input type="checkbox"/> Amended <input type="checkbox"/> Sunset/Renewal <input type="checkbox"/> Closed/Superseded	
Sequential Number	Suffix Number						
2. Agency Number	3. Unit Number						
4. RDA Status <input type="checkbox"/> New <input type="checkbox"/> Amended <input type="checkbox"/> Sunset/Renewal <input type="checkbox"/> Closed/Superseded							

5. Agency Name

Division Name	Subdivision Name
----------------------	-------------------------

6. Record Series Title

7. Record Series Life Cycle Dates	8. Medium for Records Storage – Check all appropriate categories			
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Year Created</td> <td style="width: 33%;">Year Discontinued</td> <td style="width: 33%;">Year of Final Disposition</td> </tr> </table>	Year Created	Year Discontinued	Year of Final Disposition	<input type="checkbox"/> Electronic/Digital <input type="checkbox"/> Microform <input type="checkbox"/> Paper <input type="checkbox"/> Other (Specify)
Year Created	Year Discontinued	Year of Final Disposition		

9. Retention Time Period - Specify Actual Period	10. Event that Initiates the Start of the Retention Time Period					
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">Yrs</td> <td style="width: 12.5%;">Mo</td> <td style="width: 12.5%;">Wks</td> <td style="width: 12.5%;">Days</td> <td style="width: 50%;">Permanent <input type="checkbox"/></td> </tr> </table>	Yrs	Mo	Wks	Days	Permanent <input type="checkbox"/>	Creation Fiscal Other (Specify) <input type="checkbox"/> (CR) <input type="checkbox"/> (FIS) <input type="checkbox"/>
Yrs	Mo	Wks	Days	Permanent <input type="checkbox"/>		

11. Disposition

Destroy Transfer to State Archives (WHS) Transfer to Other Location (Specify)
 Destroy Confidential Transfer to UW Archives

12. Records Series Description

<p>13. Records Contain Personally Identifiable Information (PII)</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>14. Name of Agency Program Contact or Records Officer – Select appropriate title.</p> <p style="text-align: right;"><input type="checkbox"/> Program Contact <input type="checkbox"/> Records Officer</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Telephone</td> <td style="width: 50%;">Email</td> </tr> </table>	Telephone	Email
Telephone	Email		

15. Records Series is Confidential or Access is Limited Yes No (If yes, enter Statute/Code)

16. APPROVAL SIGNATURES

Agency Official	Date (mm/dd/ccyy)	Agency Records Officer	Date (mm/dd/ccyy)
-----------------	-------------------	------------------------	-------------------

PUBLIC RECORDS BOARD APPROVAL - Contingent on restrictions to record destruction contained in s. 19.35(5), Wis. Stats., (Open Records Law), and that no records are destroyed if litigation or audit involving these records has commenced.

State Archivist	Date (mm/dd/ccyy)	Executive Secretary – PRB	Date (mm/dd/ccyy)
-----------------	-------------------	---------------------------	-------------------

INSTRUCTIONS: Records Retention/Disposition Authorization

1. **Retention/Disposition Authorization (RDA) #:**

Prior to submission to the Public Records Board (PRB) for approval, every RDA must have a unique, sequential number. Agency Records Officers generally assign this number which is subject to PRB approval. If the agency does not assign an RDA number, leave this field blank and the PRB will do so.

 - SEQUENTIAL #: Agency RDAs advance in numerical order. The Records Officer must review past RDAs and then assign the next sequential number to a new RDA.
 - SUFFIX: The Suffix is not used for most records series. It is an optional alphabetical character that may be used to indicate different retention periods, media, or dispositions for all or portions of the same records series.
2. **Agency #:** Use the following:
 - **State Agency:** Use the three-digit agency appropriation code assigned by Wis. Stats. § 20.
 - **University of Wisconsin:** Use the three-digit statutory code (285) together with the alphabetical code assigned to the institution.
 - **Local Units of Government, Other Entities:** Please contact PRB Staff.
 - **Board/Commission:** The Records Officer may assign an additional alphabetical character to autonomous entities that are attached to an agency.
3. **Unit #:** Use the following:
 - Use a 3-digit field to further indicate entity with ownership and financial responsibility for records in this series.
 - **University of Wisconsin:** Use the 6-digit UDDS # that the UW uses for accounting and budgetary purposes.
4. **RDA Status:** Check only one box:
 - NEW: Request for approval of an RDA that has never been submitted to the PRB.
 - AMENDED: Request for approval of a change to an RDA that previously was approved by the PRB. Any revision to an RDA triggers amended status with the exception of SUNSET/RENEWAL. Use existing RDA number.
 - SUNSET/RENEWAL: The RDA has sunset and is being renewed without amendments. RDA's automatically sunset every 10 years, per Wis. Stats. § 16.61(4)(c).
 - CLOSED/SUPERSEDED:
 - CLOSED: The agency no longer creates or receives records in this series. Be certain to also complete # 7, Year Discontinued and Year of Final Disposition.
 - SUPERSEDED: The RDA replaces an existing RDA, which is being superseded. If applicable, please provide the prior RDA number.
5. **Agency Name:**
 - Identify the entity that has legal custody of the records, using correct names. Do not use acronyms or abbreviations.
 - Identify the division and/or subdivision that creates and receives the records. Do not use acronyms or abbreviations.
6. **Records Series Title:**
 - Assign a descriptive title to the records series. Be certain that agency employees will be able to accurately identify the records series from its title. Do not use abbreviations or acronyms.
7. **Records Series Life Cycle Dates:** Identify the following:
 - YEAR CREATED: This is the year the agency first began creating or receiving records in this series. If the precise year is unknown, then provide an estimate.
 - YEAR DISCONTINUED: Only complete this section if the series is closed or the authority no longer has a legal obligation to create or receive records in this series.
 - YEAR OF FINAL DISPOSITION: Only complete this section of the life cycle if there is a year discontinued. The year of final disposition is the year that the agency stopped creating or receiving the records within the series plus the retention time period left for remaining records (see #9).
8. **Medium for Records Storage:** Indicate all the media on which the records are stored such as paper, electronic/digital, microform, or other, e.g. audio, film, or video. For electronic media, describe the application or file format in #12, e.g. MS Office Suite. If the original medium of an official record is converted, for example from paper to electronic, then the original may be destroyed and replaced by the new one, but only if the new medium meets all legal requirements, including those set forth in Adm 12: Electronic Records Management-Standards and Requirements.

The weblink to Adm 12 is: [Administrative Rule 12](http://www.doa.state.wi.us/category.asp?linkcatid=761&li%20nkid=127&locid=0)
<http://www.doa.state.wi.us/category.asp?linkcatid=761&li%20nkid=127&locid=0>
9. **Retention Time Period:** SPECIFY AN ACTUAL TIME PERIOD. Enter the number of years, months, weeks, or check "Permanent" to indicate period of time for retaining the records. "Permanent" means that the records need to be maintained permanently by the creating agency.
 - In # 12, provide specific justification to the PRB for the proposed retention time period. Examples of appropriate justification include, but are not limited to: citation of controlling statutes or administrative rules, consistency with related retention schedules, audit or fiscal requirements, or end of business need.
 - If a retention time period is required by law, cite the relevant statute or administrative rule in #12. If the record series is closed, specify the event that closed the file.
10. **Event:** Use this field to indicate the specific event that must occur in order to initiate the retention time period. Identify this event using one of the following terms:
 - CR: If creation of the record initiates the retention time period, mark the checkbox "CR."
 - FIS: If the retention time period is initiated by the end of a fiscal year, mark the checkbox "FIS." These records must be kept through the end of the Fiscal Year.
 - Other: If a specific event other than "CR" or FIS initiates the retention time period, mark the checkbox "Other (Specify)" and briefly describe the event. You may also provide a detailed description of the event within the Records Series Description.

INSTRUCTIONS: Records Retention/Disposition Authorization continued

- 11. Disposition:** Check the appropriate category to indicate disposition of the records after the retention time period has expired. Only one disposition may be checked. Mark as "Destroy Confidential" any record containing personally identifiable information (PII, *see* # 13, below), or information to which access is restricted by law (*see* # 16, below). If a record is marked as "Destroy Confidential," then the record destruction shall comply with all relevant legal requirements.
- 12. Records Series Description:**
- The description is the most important section of the RDA. It informs the PRB, and others who are unfamiliar with the records series, what information is contained in the series, the business purpose for the information, and the reasons why the series was created and/or received by the agency.
 - Include relevant statutory or rule citations in order to clarify the content of the records and the authorization to create them. Additional information may be included as needed for employees to manage the records, such as providing guidance regarding who is custodian of the records within the series or conditions that must be met prior to disposition, as well as the relationship to any other record series.
 - "Record series" is defined by Wis. Stats. § 16.61(2)(c).
- 13. Records Contain Personally Identifiable Information:** Check YES or NO. Wisconsin law requires authorities to specifically identify records series that contain personally identifiable information (PII). PII is defined as information that can be associated with a particular individual through one or more identifiers or other information or circumstances. Despite this broad definition, the law specifies that record series containing the following information need not be identified as PII: a) mailing lists; b) the results of certain computer matching programs; c) telephone or email directories; d) record series pertaining exclusively to agency employees; and e) those relating to procurement or budgeting.
- 14. Agency Program Contact or Records Officer:** Provide the name, telephone number and email address for the agency's statutorily-designated Records Officer or other program contact, who may be contacted for further information regarding the record series.
- 15. Records Series is Confidential or Access is Limited:**
- Check "yes" only if a specific statute or administrative rule requires that information in the record series be kept confidential or protected from public access. If "yes" is checked, identify the relevant statute or code.
 - If access to the record series is limited only to certain employees, provide written justification for limited access and identify titles of the employees who have access to the records.
 - NOTE: Some, but not all, personally identifiable information (PII) is confidential. At the same time, records that do not contain PII may be required by law to be kept confidential. For purposes of record retention and destruction, Wisconsin's Public Records Law and related statutes govern public access to records, not the designation of confidentiality.
- 16. Approval Signatures:** The Agency Records Officer, and at least one other agency official, such as the Agency Program Manager, Risk Manager, Legal Counsel, and/or the Legal Custodian of Records, must review, approve, and sign the RDA before submitting it to the PRB for approval. Prior to implementation, PRB approval and signature by the State Archivist are both required.
- 17. Contact Information:** For records management training and assistance, please contact the Wisconsin Department of Administration, Records Management Section, by telephone at: (608) 266-2995. Many records management resources are available at the Wisconsin Department of Administration website. Here are three helpful documents:
- [Statewide General Records Schedules](#)
 - http://publicrecordsboard.wi.gov/Docs_by_cat_type.asp?doccatid=678&locid=165
 - [Electronic Records and Administrative Rule 12](#)
 - <http://www.doa.state.wi.us/category.asp?linkcatid=761&li%20onkid=127&locid=0>
 - [Frequently Asked Questions](#)
 - http://www.doa.state.wi.us/faq_que_list.asp?fid=30&locid=2

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



6112 Exchange Street
McFarland, WI 53558
April 21, 2008

Michael Morgan, Secretary
Department of Administration

Karen Timberlake, Secretary
Department of Health and Family Services

Re: Open Records Request

1. Copy of current contract with Harmony Inc. for Social Assistance Management System (SAMS)
2. Copies of agendas and minutes of the Nutrition Check Committee from year 2006 to present
3. Copies of the agendas and minutes of the Data Stewardship Committee for year 2000 and a listing of meetings for years 2001 to present
4. A report on the number of nutrition participants' records contained in Wisconsin's SAMS servers

Dear Department Secretaries:

Hundreds of thousands of electronic records containing confidential information of Wisconsin's elderly and disabled citizens and their caregivers are warehoused in data centers (with suspected security vulnerabilities) outside the state of Wisconsin.

Information to populate recipients' electronic records is collected through a deceptive process that utilizes paper forms. The forms contain no mention that the information will be entered into a participant's electronic record. The attached form appears to be a self scoring stand alone checklist to be discussed with a doctor or other qualified professional rather than a form to collect information to enable electronic tracking of a client's nutrition data.

These electronic records should immediately be removed from the out of state data centers and moved to the Human Services Resource System (HSRS) at Wisconsin's data center. The secretive practice should be discontinued and only necessary information should be collected. A risk assessment as to whether security breaches might have occurred over the past several years should be conducted.

The eHealth Care Quality and Patient Safety board should consider recommending a law that would prohibit state or local agencies from circumventing ADM12, HIPAA and state privacy and open meetings laws through their placing the electronic records in data centers outside the state of Wisconsin. The principles of responsible data stewardship should be reviewed by all DHFS staff.

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.

Sincerely,

Fred Buhr, Data Entry Volunteer
McFarland Senior Outreach Program

Attachments:

Nutrition Checklist mandated to be completed by nutrition participants and entered into 25 electronic fields by the Nutrition Check Committee effective March 1, 2008

ACLU Model Standards of Fair Information Practices, all of which are violated by the Department's practice

cc: ACLU and Associated Press