



Scott Walker
Governor

Kitty Rhoades
Secretary

State of Wisconsin
Department of Health Services

DIVISION OF QUALITY ASSURANCE
1 WEST WILSON STREET
P O BOX 2969
MADISON WI 53701-2969

Telephone: 608-266-8481
FAX: 608-267-0352
TTY: 888-241-9432
dhs.wisconsin.gov

Date: April 18, 2013

DQA Memo 13-011

To: [Adult Day Care](#)
[Adult Family Homes](#)
[Community-Based Residential Facilities](#)
[Residential Care Apartment Complexes](#)

ADC 03
AFH 05
CBRF 06
RCAC 05

From: Alfred C. Johnson, Director
Bureau of Assisted Living

Via: Otis Woods, Administrator
Division of Quality Assurance

Guidelines for Use of Electronic Record Keeping in Assisted Living

The purpose of this memorandum is to provide general guidelines to assisted living providers who choose to use automated (computerized) record-keeping systems. Providers may maintain electronic or paper record systems that suit their needs as long as there is a written policy describing how state and federal regulations will be met. The guidelines below are meant to assist providers in maintaining compliance with applicable administrative code provisions but are not all-inclusive. Providers are encouraged to do further research to ensure compliance with state and federal regulations.

Electronic (Automated) Record-keeping

When automating facility records such as medical records, personnel records, resident records, training records, or any other records required by the applicable administrative code provisions, providers should consider the following:

- Protecting privacy and confidentiality
- Program oversight
- Responsibility designation
- Legal and protective measures to foster data integrity
- Record reconstruction and back up of data (in case of system failure)
- Safeguards to prevent unauthorized access

- Accessibility to authorized Bureau of Assisted Living (BAL) representatives.

For all electronic records, assisted living providers must maintain system integrity and prevent breaches of confidentiality. In an effort to meet these requirements, providers should use the following guidelines:

- Identify all personnel who have authorized access to electronic records and to what extent they have access.
- Make the application user friendly and provide proper training to personnel.
- Use a secure and unique ID number, code, password, and/or fingerprint/voice activation code to identify each authorized user. The identifiers should be complex enough and confidential so that it is known only to the user. Consider using at least eight characters, with a combination of upper and lower case letters, numbers, and symbols.
- Establish a process for verifying the accuracy of all information entered in the record, including dictation and scanned documents.
- Identify the persons responsible for the verification of information and provide a statement of their responsibilities in a signed Authorization of Use agreement.
- Incorporate a system to “flag” records with blanks, incomplete information, or questionable data before records are authenticated.
- Develop a secure method for prohibiting unauthorized changes to a record.
- Establish and enforce penalties for improper disclosure of ID numbers, codes, or passwords, or for anyone using the system without authorization. Develop protocols for how data breaches will be addressed.
- For records requiring electronic signatures, such as electronic health records (EHRs), identify all personnel by type (medical, allied health, staff, etc.) who have authorized access to modify and authenticate records.
- Retain a signed statement of authorization indicating the users’ electronic signature can only be applied to specific types or sections they have authored. System managers must have the ability to revoke this authorization at any time.
- Develop a secure method to prohibit changes to a record after being authenticated by electronic signature.
- For systems in which electronic signatures are assigned at the time of transcription, establish a way to verify the record is accurate and that the appropriate signature is assigned before it is considered complete. Normally, electronic signatures are not assigned until the author has reviewed and approved the transcription.
- Electronic health records are subject to the Health Insurance and Portability Act of 1996 (HIPAA) security and privacy rules found in 45 CFR Parts 160 and 164, as well as the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (privacy and security concerns with the electronic transmission of health

information). Educate personnel on HIPAA and HITECH security and privacy rules.
Develop a system consistent with HIPAA and HITECH requirements.

Implementing these guidelines will help providers ensure the integrity of their electronic records systems, but providers should regularly assess the system in place, continually update and educate staff, create checks and balances, and enforce penalties consistently if warranted.

Surveyor Responsibilities

In order for a CBRF or AFH to be licensed in the state of Wisconsin, it must allow the Department to “enter and inspect” the facility pursuant to Wis. Stat. § 50.03(2)(c) and (d). Per Wis. Admin. Code DHS § 89.55(1), DHS may conduct periodic inspections of a RCAC. And, per Wis. Admin. Code DHS § 106.02(9)(e)4., an ADC must permit DHS to inspect its records.

The Bureau of Assisted Living (BAL) surveyor must be able to conduct the inspection process in a consistent manner in all facilities and must be allowed access to records regardless of whether the facility uses paper or electronic records. The surveyor will cooperate with the facility to establish a process in which the surveyor will have unrestricted and timely access (within two hours) to the records. Although surveyors will make reasonable efforts to avoid the printing of entire records, printed copies may be required during an onsite survey, investigation, or follow-up visit.

The surveyor is not responsible for determining compliance with HIPAA or HITECH privacy and security rules, the legalities of disclosure requirements or business associate agreements, or the training of staff on the electronic record system. Instead, the surveyor will focus on how the electronic system is being used in the facility, effectively or improperly, in relation to the requirements for licensure or certification. For example, an unattended computer screen containing confidential information may constitute a violation of a resident’s right to privacy and confidentiality.

Goal

The goal in implementing these guidelines and understanding the role of surveyors is to keep private information secure but available to authorized individuals, and prevent sanctions for violations of state and federal regulations.

Further information about HIPAA and HITECH is available at:

- <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html>
- <http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html>