



Scott Walker
Governor

1 WEST WILSON STREET
P O BOX 2969
MADISON WI 53701-2969

Dennis G. Smith
Secretary

State of Wisconsin
Department of Health Services

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

Date: August 22, 2012

DQA Memo 12-015
Obsolete memo: DSL-BQA-00-014

To: Adult Day Care Centers	ADC	06
Adult Family Homes	AFH	08
Ambulatory Surgical Centers	ASC	04
Certified Mental Health and AODA Programs	CMHA	03
CLIA-Certified Laboratories	CLIA	03
Community Based Residential Facilities	CBRF	08
End-Stage Renal Dialysis Units	ESRD	04
Facilities Serving People with Developmental Disabilities	FDD	06
Home Health Agencies	HHA	03
Hospices	HSPCE	04
Hospitals	HOSP	06
Nurse Aide Training Programs	NATP	02
Nursing Homes	NH	10
Outpatient Rehabilitation Facilities	OPT/SP	03
Personal Care Agencies	PCP	03
Residential Care Apartment Complexes	RCAC	07
Rural Health Clinics	RHC	03

From: Otis Woods, Administrator
Division of Quality Assurance

**Requirements Regarding the Confidentiality and
Proper Disposal of Health Care and Related Records**

This memo reminds all health care providers of the statutory requirements regarding the confidentiality and proper disposal of health care and related records containing protected health information.

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security regulations establish requirements regarding the confidentiality and proper disposal of health care and related records containing protected health information (PHI). These requirements apply to all providers (who are considered “covered entities”) and their business associates who create, retain, and dispose of such records.

For providers and their business partners who are not subject to HIPAA, Wisconsin confidentiality laws have similar requirements pertaining to proper disposal of health care and related records.

HIPAA Privacy and Security Regulations

Definition of Protected Health Information

As defined in the HIPAA privacy and security regulations, PHI is protected health information (including demographic information) that:

- Is created, received, maintained, or transmitted in any form or media.
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual.
- Identifies the individual, or provides a reasonable basis to believe that it can be used to identify an individual.

A resident, client or patient name combined with his or her identification number or social security number is an example of PHI.

Requirements Regarding “Unsecured” Protected Health Information

Title XIII of the American Recovery and Reinvestment Act of 2009 (also known as the Health Information Technology for Economic and Clinical Health [HITECH] Act) included a provision that significantly expanded the scope, penalties, and compliance challenges of HIPAA. This provision imposes new requirements on covered entities and their business associates to notify patients, the federal government, and the media of breaches of “unsecured” PHI (refer to 45 CFR Parts 160 and 164 and Section 13402 of the HITECH Act).

Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of physical destruction approved by the U.S. Department of Health and Human Services (DHHS). According to the DHHS, destruction is the only acceptable method for rendering PHI unusable, unreadable, or indecipherable.

As defined by federal law, unsecured PHI includes information in *any* medium, not just electronic data.

Actions Required for Proper Disposal of Records

Under the HIPAA privacy and security regulations, health care and related records containing PHI must be disposed of in such a manner that they cannot be reconstructed. This includes ensuring that the PHI is secured (i.e., rendered unusable, unreadable, or indecipherable) prior to disposal of the records.

To secure PHI, providers and their business associates are required to use one of the following destruction methods approved by the DHHS:

- Paper, film, labels, or other hard copy media should be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed.

- Electronic media should be cleared, purged, or destroyed such that the PHI cannot be retrieved according to National Institute of Standards and Technology Special Publication 800-88, Guidelines for Media Sanitization.

For more information regarding securing PHI, providers may refer to the following Web site: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>.

Wisconsin Confidentiality Laws

Section 134.97, Wis. Stats., requires providers and their business partners who are not subject to HIPAA regulations to comply with Wisconsin confidentiality laws pertaining to the disposal of health care and related records containing PHI.

Section 146.836, Wis. Stats., specifies that the requirements apply to “all patient health care records, including those on which written, drawn, printed, spoken, visual, electromagnetic or digital information is recorded or preserved, regardless of physical form or characteristics.” Paper *and* electronic records are subject to Wisconsin confidentiality laws.

“Personally Identifiable Data” Protected

According to s. 134.97(1)(e), Wis. Stats., the types of records protected are those containing “personally identifiable data.” As defined by the law, personally identifiable data is information about an individual’s medical condition that is not considered to be public knowledge. This may include account numbers, customer numbers, and account balances.

Actions Required for Proper Disposal of Records

Health care and related records containing personally identifiable data must be disposed of in such a manner that no unauthorized person can access the personal information. For the period of time between a record’s disposal and its destruction, providers and their business partners are required to take actions that they reasonably believe will ensure that no unauthorized person will have access to the personally identifiable data contained in the record.

Businesses Affected

Sections 134.97 and 134.98, Wis. Stats., governing the proper disposal of health care and related records apply to medical businesses as well as financial institutions and tax preparation businesses. For purposes of these requirements, a medical business is any for-profit or nonprofit organization or enterprise that possesses information — other than personnel records — relating to a person’s physical or mental health, medical history, or medical treatment. Medical businesses include sole proprietorships, partnerships, firms, business trusts, joint ventures, syndicates, corporations, limited liability companies, or associates.

Continuing Responsibilities for Providers Who Cease Operations

Ceasing operations as a health care provider does not end a provider’s responsibility to protect the confidentiality of health care and related records containing PHI.

Providers who cease operations are responsible for ensuring that they and their business associates/partners continue to comply with all federal and state laws regarding protecting the confidentiality of the resident, client or patient PHI. Once record retention requirements expire, records must be disposed of in such a manner that they cannot be reconstructed, according to federal and state regulations in order to avoid penalties.

All health care providers and their business associates/partners who cease operations or go out of business should ensure that they have policies and procedures in place to protect all health care and related records from any unauthorized disclosure and use.

Penalties for Violations

Any covered entity provider or provider's business associate who violates federal HIPAA regulations regarding the confidentiality and proper disposal of health care and related records may be subject to criminal and/or civil penalties, including any or all of the following:

- Fines up to \$1.5 million per calendar year.
- Jail time.
- DHHS Office of Civil Rights enforcement actions.

For entities not subject to HIPAA, section 134.97(4), Wis. Stats., imposes penalties for violations of confidentiality laws. Any provider or provider's business partner who violates Wisconsin confidentiality laws may be subject to fines up to \$1,000 per incident or occurrence.

For more specific information on the penalties for violations related to resident, client or patient health care records, providers should refer to Section 13410(d) of the HITECH Act, amending 42 USC s. 1320d-5, and s. 134.97(3)-(4) and s. 146.84, Wis. Stats.