




Employ Milwaukee Administrative Memo		
Issue Date	07-01-2024	24-06
Sponsoring Executive	<input checked="" type="checkbox"/> Interim President and CEO	<input type="checkbox"/> CFO
Dissemination	<input checked="" type="checkbox"/> Internal	<input type="checkbox"/> External

TO: Employ Milwaukee Staff and Workforce Partners

FROM: Julie Cayo, Interim President and CEO 

RE: Protection of Confidential Information - Windows to Work

I. **BACKGROUND:** Employ Milwaukee, Inc. (EMI) contracts with the Department of Corrections (DOC) and abides by their current Executive Directives pertaining to Protection of Confidential Information. State and federal laws restrict the use or disclosure of certain types of information, such as the protected health information of Persons in our Care, juvenile justice information, and student education records. In addition, state and federal laws aimed at preventing identity theft protect personal information (also known as personally identifiable information), such as Social Security Numbers (SSN), financial account information and driver's license numbers. Furthermore, Wisconsin has a data breach notification law requiring notification of individuals whose personal information has been acquired by an unauthorized individual. EMI and DOC have a shared responsibility to maintain and protect the confidential information under its control. To prevent and mitigate the risks associated with unauthorized use or disclosure of DOC confidential information, this directive governs the protection of confidential information. Together with the DOC, EMI is committed to the principle of limited collection, access, use, disclosure, and the secure storage and disposal of confidential information.

II. **DEFINITIONS:**

- A. "Breach" means an impermissible use or disclosure that compromises the security or privacy of confidential information.
- B. "BTM" means the Bureau of Technology Management.
- C. "Confidential Information" means any communication, records, materials, and knowledge prohibited from disclosure or misuses by law, rule, order, regulation, DOC policy, or otherwise established by the Department.
- D. "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of confidential information.
- E. "Employee" means any person working at the Department of Corrections. This includes limited term employees, project and permanent employees, contractors, students, interns, and volunteers.
- F. "Encryption" means the process of changing or scrambling stored or transmitted data in order to prevent someone other than the sender and intended recipient from reading it.
- G. "HIPAA/Privacy Officer" is the DOC person who oversees the development and implementation of policies and procedures required by the HIPAA Privacy Rule. This is the DOC's primary resource for dealing with HIPAA violations throughout DOC. The position is responsible for investigating and reporting HIPAA breaches to the federal Health & Human Services Department and for providing information about

matters covered by 164.50 and responding to HIPAA complaints outside of the Inmate Complaint Review System (ICRS).

- H. "HIPAA Security Officer" means the security official who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule for the DOC. 45 C.F.R. § 164.308.
- I. "Personal Information" has the meaning under s. 134.98 (1) (b). Wis. Stat.
- J. "Person In Our Care (PIOC)" means any person who is under the supervision of the DOC either in a correctional facility or in the community including but not limited to juveniles, inmates, probationers, parolees and persons on extended supervision.
- K. "Social Security Number" or "SSN" means a unique nine-digit number issued by the Social Security Administration used primarily for tax and financial reporting purposes.
- L. "Use" means the internal sharing, employing, application, utilization, examination, or analysis of confidential information.

III. **PURPOSE:** This policy governs the protection of confidential information maintained for business purposes by the Department. Policies and procedures governing the use of Protected Health Information (PHI) are outlined in Executive Directive 35. While PHI is included in this directive, additional policies and procedures govern the use and disclosure of PHI, including Executive Directive 35, Confidentiality and Security of Health Information for Person(s) In Our care (PIOC). Violations of any of these policies must be reported to the DOC HIPAA/Privacy Officer.

- IV. **POLICY:** All services provided to DOC persons in our care are confidential in nature. EMI shall make all reasonable efforts to ensure that it or its employees and subrecipients (when applicable)
- A. Have limited collection, access, use, disclosure, and the secure storage and disposal of confidential information.
 - B. Do not disseminate such confidential information, including but not limited to identity of DOC persons in our care or services being received and to ensure that confidential information obtained through direct or indirect contact with DOC persons in our care, staff, or other parties is not disseminated without the DOC's prior permission and in a manner that complies with all applicable confidentiality laws and requirements.
 - C. No employee shall disclose confidential information unless it is permitted or required by law and there is a clear business need to do so.
 - D. No employee shall use confidential information unless it is permitted or required by law and there is a clear business need to do so.

This directive does not supersede any Wisconsin, federal or local law relating to the collection, handling, maintenance, disposal, or breaches of confidential information.

V. **PROCEDURES**

- A. All Windows to Work employees will be required to complete privacy security training provided by the DOC's Division of Management Services (DMS) whom develops standards for managing confidential information to include the following:
 - i. Collection
 - ii. Access

- i. Use
- ii. Disclosure.
- iii. Secure storage and disposal
- iv. Reporting and responding to breaches of confidential information

VI. Action Required

- A. Posting of this Admin Memo to the Employ Milwaukee website for open access to all personnel.
- B. The EMI Program Manager will document Windows to Work employee completion of privacy security training provided by the DOC's DMS.

REFERENCES:

- Wis. Stats. §§ 19.36 (10), 103.13 (6), and 230.13
- Wis. Stat. § 51.30(4) Wis. Stat. § 252.15(3m)
- Wis. Stat. § 118.125
- Wis. Stat. § 134.98 Wis. Stat. § 938.78
- Wis. Stats. §§ 146.81 - 146.84
- Wisconsin Administrative Code Ch. DOC 310
- Wisconsin Administrative Code Ch. DOC 380
- Wisconsin Administrative Code Ch. DOC 396
- 5 U.S.C. § 552a
- 18 U.S.C. § 1028
- 20 U.S.C. § 1232g
- 29 U.S.C. Chapter 28
- 42 U.S.C. § 405(c)(2)(C)(i)
- 42 U.S.C. §. 12101 Americans with Disabilities Act
- 28 C.F.R. 0, I, pt 20 42 U.S.C. § 12101
- 34 C.F.R. § 99
- 42 C.F.R. Part 2
- 42 C.F.R. Parts 160, 162, and 164
- DOC ED 35 - Confidentiality and Security of Health Information for Person(s) in Our Care (PIOC)
- DOC ED 50 - Appropriate Use of Technology Resources
- The Secretary of the Department of Corrections (DOC), as the head of a principal administrative agency within the executive branch of Wisconsin state government, has the power and duty to issue an executive directive to plan, direct, coordinate and execute the functions vested in the agency in carrying out programs and policies within the limits established by the legislature under
 - s. 15.001 (1),
 - s 15.01 (5),
 - s. 15.01 (8),
 - sr. 15.04 (1) (a) and s. 15.14, Wis. Stats.

REVISIONS: None