DIVISION OF ADULT INSTITUTIONS **POLICY AND PROCEDURES**	**DAI Policy #:** 500.50.21	**Page** 1 of 6
	Original Effective Date: 10/26/11	**New Effective Date:** 08/06/24
	Supersedes: 500.50.21	**Dated:** 01/11/21
	Administrator's Approval: Sarah Cooper, Administrator – 07/15/24	
	Required Posting or Restricted: [x] **Inmate** [x] **All Staff** [ ] **Restricted**	
Chapter: 500 Health Services		
Subject: Confidentiality of Health Care Record		

POLICY

The Division of Adult Institutions shall maintain the confidentiality of PIOC written or electronic health record, as well as verbally conveyed health information, pursuant to federal and Wisconsin laws and Department of Corrections policies.

REFERENCES

Standards for Health Services in Prisons, National Commission on Correctional Health Care, 2018, P-A-08 Health Records
Federal Regulations, 42 CFR Part 2 – Confidentiality of Alcohol and Drug Abuse Patient Records
Federal Regulations, 45 C.R.R., Parts 160, 162, and 164, HIPAA Regulations
Wisc. Stat. s. 146.83 – Access to patient health care records
Wisc. Stat. s. 252.15 – Restrictions on use of an HIV test
Executive Directive 35 – Confidentiality of Offender Health Care Information
Executive Directive 50 – Use of DOC Information Technology Resources
DAI Policy 500.10.36 – Responsible Health Authority
DAI Policy 500.50.01 – Minimum Necessary and Duty to Mitigate HIPAA Standards
DAI Policy 500.50.06 – Management of DOC Health Care Records
Human Resources Policy 200.30.014 – Telecommuting/Work from Home Policy

DEFINITIONS, ACRONYMS AND FORMS

BHS – Bureau of Health Services

DAI – Division of Adult Institutions

DOC – Department of Corrections

DOC-2925 – Remote Work Agreement

Health Care Record (HCR) – Official confidential DOC record created and maintained for each PIOC consisting of all or some of the following components: Medical Chart, Dental Services Record, Dialysis Chart, Psychological Records-Copies envelope, Medications Record envelope, Patient Request Folder, Psychological Services Unit Record, Psychological Services Unit Record – Alcohol and Other Drug Abuse (AODA) envelope and other components as defined by the BHS.

HIPAA – Health Insurance Portability and Accountability Act

Responsible Health Authority (RHA) – The designated health authority responsible for overseeing the delivery of health care services.

PIOC – Persons in our care

RDA - Records Disposition Authorization

WICS – Wisconsin Integrated Corrections System

PROCEDURES

I. General Guidelines

A. The DOC Health Information Supervisor and HIPAA/Privacy Compliance Officer shall:
   1. Keep the RHA/designees informed about all Wisconsin and federal confidentiality laws and changes to those laws.
   2. Work with RHA/designee to ensure policies are created and revised, as necessary, to comply with Wisconsin and federal confidentiality laws.
   3. Develop and update training related to the laws.

B. Training related to security, confidentiality, and incident reporting of HCR and HIPAA data will occur at the work site and under the direction of the immediate supervisor.

C. Records shall be maintained which document that all staff have received instruction about the confidentiality of HCRs and health information at a minimum at BHS New Employee Orientation, in the minutes at staff meetings, and at other training sessions. Documentation of healthcare staff instruction on maintaining confidentiality shall be retained according to the defined RDA.

II. Access Establishment and Modification

A. All requests for access to the Electronic Medical Record (Cerner) shall be submitted on a DOC-5600 “Employee Access and Equipment Request” and approved by the requestor’s immediate supervisor.
   1. The immediate supervisor is responsible for notifying the BTM immediately of employees transferred into a new department, staff with a new role or those terminated through the submission of a “DOC-5600 Employee Access and Equipment Request”.
   2. The BTM Identity and Access Management Team is responsible for changing the user’s access to the EMR based on the user’s new role within 10 business days of notification.

B. Workforce Clearance Procedures
   1. The EMR role assigned to a user is based on the minimum necessary information (amount of data) access required to carry out legitimate job

responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
2. All access requests are processed so as to provide the necessary level of access while also adhering to the minimum necessary requirements of the Privacy Rule. Blanket access is not provided for any user.
3. Any access not specifically authorized is prohibited.

C. Remote Access Authorization
1. Employees utilizing the EMR outside of the facility shall keep secure all records to ensure there are no privacy breaches.
2. Remote access to health records through telecommuting shall be granted by the immediate supervisor utilizing the DOC-2925 – Remote Work Agreement.
3. Guidelines for telecommuting are established within the Human Resources Policy 200.30.014.

D. Unique User Identification and Authentication
1. Access to the organization's EMR application is controlled by requiring a unique User Login ID and password for each authorized user.
2. Users shall not select passwords that may be easily guessed or obtained using personal information (i.e., names, favorite sports team).
3. User Login IDs and passwords are used to control access to the organization's EMR and should not be disclosed.
4. Users shall not allow anyone for any reason to have access to the user's unique User Login ID and password.
5. Users shall never login for someone else, in violation of Executive Directive 50.
6. The EMR automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the ePHI contained within the application.
7. Users that do not recall their password may contact the BTM Help Desk. for assistance.
8. If a user believes their User Login ID has been compromised, they are required to immediately report the incident to the BTM Help Desk.

E. Automatic Logoff
1. Users are required to make the EMR inaccessible by any other individual when unattended (i.e., locking or logging off the systems; if the device is used only by a single individual with a unique log in, it may be locked).
2. Users must log off the EMR application at the end of their shift, or at the end of their need to use the application, whichever is sooner. Users shall complete this activity on each workstation they have logged into.
3. The EMR will automatically log users off the systems after 5 minutes of inactivity.

F. Computer Workstation Use

1. Computer workstations shall only be used for authorized business purposes.
2. When possible, workstations shall be placed in secure areas. Workstations in exam rooms or public areas must be logged off or locked when not in use. Users must take actions to prevent unauthorized viewing (e.g., privacy screens, minimizing sessions, closing laptops, positioning screens away from public view).
3. All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI in the EMR application at all times.
4. Workstations may not be used to engage in any activity that is illegal or is in violation of DOC policies.

G. Termination Procedures
   1. The DOC-5600 form shall be used to initiate a termination. This will initiate the following activities:
      a. The Human Resources Department (or other designated department), users, and their supervisors are required to notify BTM Security upon completion and/or termination of access needs.
      b. The Human Resources Department, users, and supervisors are required to notify BTM to terminate a user's access rights if there is evidence or reason to believe the following and are filed with the Privacy Officer (these incidents are also reported on an incident report within WICS):
         i. The user has been using their access rights inappropriately.
         ii. A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password).
         iii. An unauthorized individual is using a user's Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
   2. The BTM Identity and Access Management Team shall terminate users' access rights as soon as reasonably possible upon notification.
   3. The HIPAA Security officers shall audit termination of access on a quarterly basis, and may terminate access of users that have not logged into organization's information systems/applications for a period of over six (6) months.

DIVISION OF ADULT INSTITUTIONS FACILITY IMPLEMENTATION PROCEDURES

Facility: Name		
New Effective Date: 00/00/00	**DAI Policy Number:** 500.50.21	**Page** 6 of 6
Chapter: 500 Health Services		
Subject: Confidentiality of Health Care Record		

REFERENCES

DEFINITIONS, ACRONYMS AND FORMS

FACILITY PROCEDURE

I.

A.

B.

1.

2.

a.

b.

c.

3.

C.

II.

III.

RESPONSIBILITY

I. Staff

II. Inmate

III. Other