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:** 01/11/21
	Supersedes: 500.50.21	**Dated:** 06/01/16
	Administrator's Approval: Makda Fessahaye, Administrator	
	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 a patient's 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 16, HIPAA Regulations
Wisconsin Statutes s. 146.83 – Access to patient health care records
Wisconsin Statutes s. 252.15 – Restrictions on use of an HIV test
Executive Directive 35 – Confidentiality of Offender Health Care Information
DAI Policy 500.50.01 – Minimum Necessary and Duty to Mitigate HIPAA Standards
DAI Policy 500.50.06 – Management of DOC Health Care Records

DEFINITIONS, ACRONYMS AND FORMS

BHS – Bureau of Health Services

DAI – Division of Adult Institutions

DOC – Department of Corrections

Health Care Record (HCR) – Official confidential DOC record created and maintained for each patient 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 – AODA envelope and other components as defined by the BHS.

HIPAA – Health Insurance Portability and Accountability Act

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

UPS – United Parcel Service

USPS – United States Postal Service

PROCEDURES

I. General Guidelines

A. The Health Information Supervisor/HIPAA Compliance Officer shall:
   1. Keep the RHA/designees informed about all Wisconsin and federal confidentiality laws and changes to those laws.
   2. Create and revise policies to implement the laws.
   3. Develop and update training related to the laws.

B. DAI shall maintain records 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.

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" approved by the requestor's immediate supervisor.
   1. Training related to security, confidentiality and incident reporting will occur at the work site and under the direction of the immediate supervisor.
   2. The "DOC-5600 Employee Access and Equipment Request" is maintained by the Bureau of Technology Management (BTM) Security Team.

B. The immediate supervisor is responsible for notifying the BTM of employees transferred into a new department or new role and facilitating completion of the "DOC-5600 Employee Access and Equipment Request".
   1. The BTM Security Team is responsible for changing the user's access to the EMR based on the user's new role within 5 business days of notification.

C. 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.

D. Access Authorization
   1. Role based access categories for each information system/application are pre-approved by the immediate supervisor. Access shall be based on the minimum necessary information needed for the user's role.

2. The BTM Security Team grants the level of access to users based on these pre-determined categories.
3. Refer to the remote access policy for details relating to remote access.
4. Requested access will be audited quarterly by the HIPAA Privacy Officer and the HIPAA Security Officer to ensure appropriateness of higher levels of access.

E. Person or Entity Authentication
Each user has and uses a unique User Login ID and password that identifies and authenticates him/her as the user of the information system.

F. Unique User Identification
1. Access to the organization's EMR application is controlled by requiring a unique User Login ID and password for each authorized user.
2. Password requirements are enforced by the BTM.
3. Users shall not select passwords that may be easily guessed or obtained using personal information (i.e., names, favorite sports team)
4. The BTM Security Team assigns User Name and generic password for each user to utilize for first time access into each information system. The User Login ID and password are forwarded to the user securely.
5. The EMR shall automatically require users to change their password upon first-time use of the information system.

G. Password Management
1. User Login IDs and passwords are used to control access to the organization's EMR and should not be disclosed.
2. Users shall not allow anyone for any reason to have access to the user's unique User Login ID and password.
3. Users shall never login for someone else, in violation of ED 50.
4. 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.
5. Users that do not recall their password may contact the BTM Help Desk. The BTM Help Desk provides the employee with a temporary, one-time use password which must be changed on first use.
6. Passwords are inactivated upon an employee's termination (refer to the termination procedures in this policy).
7. If a user believes their User Login ID has been compromised, they are required to immediately report the incident to the Help Desk.

H. Automatic Logoff
1. Users are required to make the EMR inaccessible by any other individual when unattended by the users (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.

3. The EMR will automatically log users off the systems after 5 minutes of inactivity.

I. Workstation Use
1. Workstations shall only be used for authorized business purposes.
2. When possible, workstations shall be placed in secure areas. Workstations in patient 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.

J. Termination Procedures
The DOC-5600 form will be used to initiate a termination. This will initiate the following activities:
1. 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.
2. The Human Resources Department, users, and supervisors are required to notify BTM Security 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 (WICS):
    1. The user has been using their access rights inappropriately.
    2. 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).
    3. 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).
3. BTM Security will terminate users' access rights immediately upon notification.
4. The HIPAA Privacy and Security officers will audit 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.

Bureau of Health Services: Michael Rivers **Date Signed:** 1/8/21
Michael Rivers, Director of Healthcare Administration

_____ **Date Signed:** _____
Vacant, Medical Director

Mary Muse **Date Signed:** 1/8/21
Mary Muse, Nursing Director

Administrator's Approval: _____ **Date Signed:** 01/11/21
Makda Fessahaye, Administrator

DIVISION OF ADULT INSTITUTIONS FACILITY IMPLEMENTATION PROCEDURES

Facility: Name		
Original Effective Date:	**DAI Policy Number:** 500.50.21	**Page** 6 of 6
New Effective Date: 00/00/00	**Supersedes Number:**	**Dated:**
Chapter: 500 Health Services		
Subject: Confidentiality of Health Care Record		
Will Implement ☐ As written ☐ With below procedures for facility implementation		
Warden's/Center Superintendent's Approval:		

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