



Department: Human Resources
Policy Number: OSM-A002
Effective Date: 02/01/2018

ADMINISTRATIVE POLICY

The online version of this policy is official.
Therefore, all printed versions of this
document are unofficial copies.

PHI / HIPAA POLICY (Protected Health Information/Health Insurance Portability & Accountability Act)

Objective

CMCSS has adopted a policy that protects the privacy and confidentiality of protected health information (PHI) whenever it is used by its' representatives. The private and confidential use of such information will be the responsibility of all individuals with job duties requiring access to PHI in the course of their jobs.

Protected Health Information Defined

PHI refers to individually identifiable health information received by the CMCSS / County group health plan or received by a health care office, health care provider, health plan or health care clearinghouse that relates to the past or present health of an individual or to payment of health care claims. PHI information includes medical conditions, health status, claims experience, medical histories, physical examinations, genetic information and evidence of disability.

The HIPAA Compliance Officer

CMCSS has designated the Onsite Clinic Manager as the PHI / HIPAA compliance officer (HCO), and any questions or issues regarding PHI should be presented to the HCO for resolution. The HCO is also charged with the responsibility for:

- Issuing procedural guidelines for access for PHI. Refer to OSM-P001
- Developing a matrix for personnel who will need access to PHI. Refer to OSM-G014
- Developing guidelines for describing how and when PHI will be maintained, used, transferred, or transmitted. Refer to OSM-P002

Records Retention

Personnel records and disclosures of PHI will be maintained as required by state and federal law. Records that have been maintained for the maximum interval will be destroyed in a manner to ensure that such data are not compromised in the future in accordance with the CMCSS record destruction policy.

Annual Activities Necessitating Use of PHI

Annually or more frequently as necessary, CMCSS performs enrollment, changes in enrollment and payroll deductions; provides assistance in claims problem resolution and explanation of benefits issues; and assists in coordination of benefits with other providers. Some or all of these activities may require the use or transmission of PHI. Thus, all information related to these processes will be maintained in confidence, and employees will not disclose PHI from these processes for employment-related actions, except as provided by administrative procedures approved by CMCSS. Employees who have access to PHI must sign a HIPAA confidentiality statement (OSM-F060) and adhere to the guidelines at all times. Business associates of the Onsite Medical Clinic who access PHI must sign the guidelines as stated in the Business Associate Agreement (OSM-F059) and these guidelines should be adhered to at all times. General rules regarding PHI are as listed below:

- Disclosures that do not qualify as PHI-protected disclosures include:
 - Disclosure of PHI to the individual to whom the PHI belongs.
 - Requests by providers for treatment or payment.
 - Disclosures requested to be made to authorized parties by the individual PHI holder.
 - Disclosures to government agencies for reporting or enforcement purposes.



- Disclosures to workers' compensation providers and those authorized by the workers' compensation providers.
- Information regarding whether an individual is covered by a plan for claims processing purposes may be disclosed.
- Information external to the health plan is not considered PHI if the information is being furnished for claims processing purposes involving workers' compensation or short- or long-term disability and medical information received to verify Americans with Disabilities Act (ADA) or Family and Medical Leave Act (FMLA) status.

Use of the online Electronic Health Record (EHR) by the Onsite Medical Clinic requires users to maintain a username and password. This information is not to be shared with any other individuals. The Onsite Clinic Manager will monitor on a monthly basis and verify appropriate access to the EHR by all individuals. When an employee's Onsite relationship is on a hiatus of over 90 days (i.e. employee is a summer employee), their EHR access will be made "inactive" until their relationship is in current use. When an employee's Onsite employee relationship is terminated, the individual's access to the EHR will be terminated.

Implementing Procedures:

[OSM-P002](#) Procedural Guidelines for PHI access

[OSM-P003](#) Procedural Guidelines for Maintenance, Use, or Transferring / Transmitting of PHI

Associated Documents:

[OSM-F059](#) HIPAA Business Associate Agreement

[OSM-F060](#) HIPAA / Medical Information Confidentiality Agreement (Onsite)

[HUM-F094](#) HIPAA / Medical Information Confidentiality Agreement (Human Resources)

[OSM-G014](#) Role Based Matrix for PHI

[OSM-NOPP](#) Notice of Privacy Practices

Revision History:

<u>Date:</u>	<u>Rev.</u>	<u>Description of Revision:</u>
02/01/18		Initial Release

***** End of Policy *****