Information Access Management Policy

PURPOSE
In recognition of the critical role that information systems play in COMPANY Corporation ("COMPANY") business activities, this policy defines the Health Insurance Portability and Accountability Act (along with its subsequent amendments "HIPAA") Security Rules Administrative Safeguards (45 C.F.R.164.308) and other requirements necessary for the secure handling and storage of electronic protected health information ("ePHI"). This policy defines administrative safeguards that everyone at COMPANY is expected to be familiar with and to consistently follow.

Note: HIPAA Policies and supporting documents are supplemental to COMPANY's Employee Handbook, the terms of which are incorporated herein by reference, and is intended to be read in concert with the same. In the event any terms appear to conflict, please see your supervisor for clarification.

SCOPE
These policies apply to all COMPANY Personnel.

COMPANY's Information Security Officer ("ISO") owns and is responsible for updates, enforcement, and exceptions and may be appropriately delegated only to specified, qualified individuals. Department heads are responsible for ensuring their department Personnel are complying with all applicable policies and procedures, addressing non-compliance, and informing the ISO (or delegate) of issues when appropriate.

DEFINITIONS
COMPANY means COMPANY Corporation.

HIPAA means the Health Insurance Portability and Accountability Act, along with its subsequent amendments.

Personnel means all employees, consultants, contractors, and volunteers who perform work directly for COMPANY and not through an intermediary.

PHI means protected health information as defined under HIPAA.

POLICY
"Required" and "Addressable" are defined under HIPAA.

Company shall implement policies and procedures to prevent, detect, contain, and correct security violations. 45 C.F.R.164.308(a)(4).

COMPANY shall implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the HIPAA Privacy Rule.

Specifically, COMPANY shall undertake the following activities and processes:

- Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.

- Access authorization (Addressable). Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

- Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. As applicable, COMPANY may notify law enforcement authorities of any suspected or actual unlawful activity and to cooperate in any investigation of such activity. Conduct in violation of this policy is not within the course and scope of employment. Therefore, COMPANY reserves the right not to defend or pay any damages awarded against Personnel that result from violation of this policy.

Any Personnel who is requested to undertake an activity which he or she believes is in violation of this policy or observes potential violations, must notify the ISO or the legal team immediately.

RELATED DOCUMENTS/ATTACHMENTS

COMPANY should list any related documents here or in a master document list.

HISTORY

Version	Description/Action	Date	Reviewer(s)
.00	All HIPAA policies reviewed and revised.		Executive Management General Counsel VP, AGC Privacy & Compliance Information Security Officer