Title: HIPAA Security Policy	Reference #: HA002
Section:	Date Effective/Revised: 3/15/2024
Department (s): Healthcare Components	Approved By: Board of Supervisors

GENERAL SECURITY COMPLIANCE

Iowa County is committed to conducting business in compliance with all applicable laws, regulations, and policies. Iowa County has adopted this policy to set forth its compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of Electronic PHI ("ePHI")(the "Security Regulations").

This Policy covers Iowa County's approach to compliance with the Security Regulations. As a covered entity under the Security Regulations, Iowa County must:

(1) Ensure the confidentiality, integrity, and availability of all ePHI Iowa County creates, receives, maintains or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and

(4) Ensure compliance with the Security Regulations by its Workforce.

Compliance with the Security Regulations will require Iowa County to implement:

Administrative Safeguards--those actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of the Iowa County's Workforce in relation to the protection of and authorized access to said ePHI.

Physical Safeguards--those physical measures, policies and procedures to protect Iowa County's electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Technical Safeguards--the technologies and the policies and procedures for its use that protect ePHI and control access to it.

The Security Regulations permit Iowa County to implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Regulations. In determining which security measures to implement, Iowa County has taken into account its size, complexity and capabilities; technical infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to ePHI. Iowa County has departments who have different uses of PHI for Iowa County. These departments will be referred to in this Security Policy as "Departments". In the Security Policy, Iowa County

Title: HIPAA Security Policy	Reference #: HA002
Section:	Date Effective/Revised: 3/15/2024
Department (s): Healthcare Components	Approved By: Board of Supervisors

has determined that Departments in some cases must implement a particular security measure and in other cases have discretion to determine which security measures to implement.

HIPAA Compliant Cloud Storage

All Iowa County Healthcare components use HIPPA Compliant Cloud Storage to store and access PHI. Iowa County does not store and should not store any PHI on local servers unless it is encrypted and HIPPA compliant.

Any service provider offering a HIPAA-compliant cloud storage service must ensure multiple safeguards are implemented to ensure sensitive data is protected at all times. Robust access controls must be in place, event logging is required to maintain an audit trail, and the hosting provider must conduct regular, rigorous assessments to ensure its platform remains secure and in compliance with HIPAA.

In addition to stringent privacy and security controls, hosting providers are required to sign a business associate agreement with Iowa County.

The HIPAA Security Rule requires cloud storage services to include safeguards to ensure the privacy and security of healthcare data, but also to ensure that information is always available. A HIPAA cloud storage solution must have near- 100% uptime to ensure ePHI can always be accessed, along with robust backup policies to ensure data can be recovered in the event of disaster.

All cloud storage platforms must satisfy all relevant provisions of the HIPAA Privacy and Security Rules before it can be used in connection with any ePHI. HIPAA requires covered entities to obtain reasonable assurances that a service provider is in compliance with HIPAA.

All cloud storage platforms must ensure data is encrypted at rest and in transit to the standard recommended by the National institute of Standards and Technology (NIST) and data is stored in secure data centers.

Title: HIPAA Security Policy	Reference #: HA002
Section:	Date Effective/Revised: 3/15/2024
Department (s): Healthcare Components	Approved By: Board of Supervisors

ASSIGNED SECURITY RESPONSIBILITY POLICY

POLICY

On behalf of its covered entity component parts, Iowa County has designated a HIPAA Committee with overall responsibility for the development and implementation of policies that conform to the Security Regulations, and to provide strategic direction and tactical management to ensure the security, confidentiality, availability, and integrity of ePHI.

The HIPAA Committee will consist of the Department Head or their Designee from the following healthcare components.

- EMS & Safety Director (chairperson)
- Public Health Director
- Board of Supervisors Member
- Iowa County Auditor
- Iowa County Transportation Director
- Veterans Affairs Director
- Mental Health/Social Services Representative

PURPOSE

The purpose of this policy is to establish the duties and responsibilities of the HIPAA Committee and each Department HIPAA Security Liaison.

PROCEDURES

1) The HIPAA Committee shall oversee the development, implementation, and operation of Iowa County's HIPAA Security Program. The HIPAA Committee shall have the following responsibilities:

    a) Develop and revise as needed these HIPAA Security Policies and Procedures and other mechanisms as necessary to address identified security threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
    b) Answer all questions from employees concerning the ePHI security safeguards, policies and procedures that are not adequately addressed by immediate supervision.
    c) Prepare cost benefit analyses of appropriate ePHI safeguards and make recommendations to management regarding the adoption of safeguards.
    d) Prepare the annual budgets for ePHI security.
    e) Meet with appropriate Individuals, including IT services, the Privacy Officer and the Board of Supervisors periodically, to discuss ePHI security issues, policies and planning.

Title: HIPAA Security Policy	Reference #: HA002
Section:	Date Effective/Revised: 3/15/2024
Department (s): Healthcare Components	Approved By: Board of Supervisors

f) Ensure that all ePHI security policy and procedure manuals and materials are kept up to date and current with government rules, regulations, and practices.

g) Monitor Iowa County's compliance with applicable ePHI security laws and regulations; monitor compliance with these HIPAA Security Policies and Procedures among Iowa County's employees and other third parties, and refer issues to appropriate managers or administrators;

h) Maintain records of access authorizations and document and review the levels of access granted to a user, program, or procedure accessing ePHI on an ongoing basis.

i) Prepare and periodically assess Iowa County's security incident response procedures, disaster recovery plan and business continuity plan for information systems containing ePHI;

j) Perform security audits and risk assessments of ongoing system activities utilizing ePHI.

k) Provide consulting support and make recommendations to the Board of Supervisors regarding appropriate, timely and necessary improvements or enhancements to the ePHI security program.

l) Coordinate ongoing review of existing ePHI security programs and initiate the development of new programs, as needed.

m) Investigate ePHI system security breaches, and, in consultation with the Privacy Officer and IT Services, and administer appropriate sanctions related to security violations; and

n) Facilitate a process for individuals to file a complaint regarding the Iowa County's Security Policies or the handling of ePHI by a Covered Entity HIPAA health care component, including ensuring that the complaint and its disposition are appropriately documented and handled.