HIPAA Policy - KnowCode

Effective Date: 05/07/2024

KnowCode, a unit of DigitalSquad LLC ("KnowCode," "we," "our," or "us"), is committed to maintaining the privacy, security, and confidentiality of Protected Health Information (PHI) as required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These HIPAA Policies outline how KnowCode complies with HIPAA regulations to protect PHI across our Services, including design, development, digital marketing, BPO, KPO, and other offerings.

---

1. Scope

These HIPAA Policies apply to all employees, contractors, and partners of KnowCode who handle or have access to PHI as part of providing services to clients in the healthcare industry.

---

2. Definitions

- **Protected Health Information (PHI):** Any information related to an individual's health status, provision of healthcare, or payment for healthcare that can be linked to a specific individual.
- **Business Associate:** KnowCode acts as a Business Associate when working with Covered Entities (e.g., healthcare providers, health plans).
- **Covered Entity:** Healthcare providers, health plans, or clearinghouses that transmit PHI electronically.

---

3. HIPAA Compliance Requirements

3.1 Privacy Rule

- **Access and Use of PHI:** KnowCode employees and contractors may only access PHI as required to perform contracted services.
- **Minimum Necessary Standard:** Only the minimum necessary amount of PHI will be accessed or disclosed to fulfill service obligations.
- **Client Agreements:** KnowCode will execute Business Associate Agreements (BAAs) with all Covered Entities to outline roles and responsibilities regarding HIPAA compliance.

3.2 Security Rule

We implement administrative, physical, and technical safeguards to ensure the security of electronic PHI (ePHI):

- **Administrative Safeguards:**
    - Conduct risk assessments to identify vulnerabilities.
    - Develop and enforce policies for handling PHI securely.

    - Provide HIPAA training to all employees and contractors.
- **Physical Safeguards:**
    - Secure all facilities and devices where ePHI is stored.
    - Implement access controls to restrict unauthorized entry.
- **Technical Safeguards:**
    - Use encryption for data transmission and storage.
    - Implement secure authentication methods for accessing systems.
    - Regularly update and patch software to prevent security breaches.

3.3 Breach Notification Rule

- **Breach Identification:** A breach is defined as the unauthorized access, use, or disclosure of PHI that compromises its security or privacy.
- **Notification Timeline:** In the event of a breach, KnowCode will notify affected Covered Entities within the timeframe specified by HIPAA regulations (typically no later than 60 days from discovery).
- **Mitigation Efforts:** We will take immediate steps to contain and mitigate any breach, including notifying impacted individuals if required.

---

4. Responsibilities of Employees and Contractors

- **Training:** All employees and contractors must complete mandatory HIPAA training and adhere to KnowCode's policies.
- **Confidentiality Agreements:** Employees and contractors must sign confidentiality agreements acknowledging their responsibilities under HIPAA.
- **Incident Reporting:** Any suspected or actual breach of PHI must be reported immediately to the designated HIPAA Compliance Officer.

---

5. Data Handling and Retention

- **Data Storage:** PHI must be stored in secure, HIPAA-compliant systems with access controls.
- **Data Transmission:** PHI transmitted electronically must be encrypted using industry-standard protocols.
- **Retention Period:** PHI will be retained only as long as necessary to fulfill contractual obligations or comply with legal requirements.
- **Data Destruction:** PHI will be securely destroyed using approved methods (e.g., shredding, wiping) once retention is no longer required.

---

6. Third-Party Vendors

Any third-party vendor engaged by KnowCode that handles PHI must:

- Sign a Business Associate Agreement (BAA).
- Demonstrate compliance with HIPAA standards.

---

7. Risk Management and Audits

- **Risk Assessments:** Regular risk assessments will be conducted to identify and address potential vulnerabilities in handling PHI.
- **Internal Audits:** Periodic audits will be performed to ensure compliance with HIPAA policies and regulations.
- **Corrective Actions:** Any identified compliance gaps will be addressed promptly with corrective measures.

---

8. HIPAA Compliance Officer

KnowCode has designated a HIPAA Compliance Officer responsible for:

- Overseeing HIPAA compliance efforts.
- Providing training and support to employees.
- Investigating and responding to incidents involving PHI.
- Serving as the primary point of contact for HIPAA-related inquiries.

---

9. Disciplinary Actions

Non-compliance with these HIPAA Policies may result in disciplinary actions, including but not limited to:

- Verbal or written warnings.
- Suspension or termination of employment or contract.
- Legal actions if necessary.

---

10. Updates to HIPAA Policies

These policies may be updated periodically to reflect changes in regulations or operational requirements. Updates will be communicated to all employees, contractors, and clients.

---

11. Contact Information

If you have questions about our HIPAA Policies or suspect a breach of PHI, please contact:

HIPAA Compliance Officer
KnowCode (DigitalSquad LLC)
4108 Redan Rd. Ste. A3,
Stone Mountain, GA - 30083
Phone: (404) 984-2226
Email: compliance@knowcode.us