TriageLogic
TriageLogic Group
WHEN PATIENTS CALL, WE'RE YOUR ANSWER

TriageLogic Information Security Policy

What is HIPAA, and what information is protected by it?
HIPAA, short for the United States Health Insurance Portability and Accountability Act, is a set of standards introduced by Congress in 1996 that aim to protect the privacy of patient information in the healthcare industry by regulating how providers handle patient data while conducting business, as well as ensuring the continuity of individuals' healthcare coverage.

There are two sections to the standard: HIPAA Title I, which focuses on protecting citizens' healthcare coverage if they are fired or laid off, and HIPAA Title II, which is focused more on patients' rights and how to properly transmit, share and store their information.

HIPAA created a set of universal standards for exchanging and securing personal data via electronic data interchange (EDI), the goal being to protect all data that is personally identifiable to a specific person, regardless if it is communicated orally, electronically or in writing.

The HIPAA privacy rule requires all health care providers, or any other organization that processes medical records, inform patients of their privacy rights, educate and train staff on how medical data should be properly handled, and implement and practice the required privacy and security policies in order to ensure that electronic health information of patients remain secure.

Breaking down HIPAA security rules and compliance guidelines
HIPAA's standards require that all health care industries apply and enforce certain protections. The implementation process will be different for every organization depending on its size, budget, risks and infrastructure complexity. But regardless of each organization's different needs in terms of HIPAA implementation, the general HIPAA requirements stay the same.

- Organizations must have an administrative authority in charge of managing and enforcing HIPAA compliance rules, regulations and efforts. There should be a clear set of guidelines in place regulating who is and isn't permitted to access patient information. All access to sensitive data and systems should be monitored.
- Documentation should be provided to patients informing them of their rights.
- All corporate systems, machines and buildings must have physical and technical data and intrusion protection controls to prevent malicious hacker and unauthorized access.
- There must be a traffic-monitoring device, such as a firewall, in place to examine activity coming into and leaving the organization's network.
- Management should practice risk assessments, data handling policies, data loss prevention (DLP) and record all security policies and procedures

Policy on Emails and other forms of communication
Email is not secure. TriageLogic requires that email **cannot** contain PHI anywhere in the heading or body of the message. To view any PHI, the user has to log into the system with a user

name and password. When communicating about patients via email, we refer to ticket numbers or note numbers without mentioning any PHI. Reports and recordings are sent as links for which the user has to login to view the PHI.

None of the following items can be included in any unsecure communication

1. Names
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data
19.

A. Policy on Printing Documents with PHI

The TriageLogic platform is a web based system. All data remains on the secure servers and requires appropriate role based access with a user name and password to access the data.

All users of the system are NEVER required to print any information based on standard workflows. Users are NOT PERMITTED to print any information.

If the user needs to make notes about a patient, then they must use a note number as a reference and omit any PHI on the written notes.

In the unusual event that patient documents need to be printed, the Director of nursing/Nurse manager is the only one that is permitted to print information from the system with PHI. Any management staff who are permitted to print PHI have a criss cross shredder at their desk to immediately shred the information after use.

B. Policy on removing PHI or other data from a computer CORE 13

The TriageLogic platform is a web based system. All data remains on the secure servers and requires appropriate role based access with a user name and password to access the data.

All users of the system are NEVER required to save any information based on standard workflows.

Users are NOT PERMITTED to save any patient data to their local computer. In the event that a computer needs to be replaced or an user leaves the company, the IT relations manager will coordinate a webex with a member of the IT team. The IT representative will access the users computer and remove all relevant data based on the latest standards of IT security.

TriageLogic HIPAA Compliance Policy

(Updated May 2018) – to be signed by all personnel with access to patient information

This **TRIAGE HIPAA COMPLIANCE POLICY** of Triage Logic Management & Consulting, LLC ("Triage") shall apply to all employees of Triage, agents of Triage and employees of Triage subcontractors (collectively the "Service Providers").

PURPOSE OF THIS POLICY. Service Providers are providing various health care services for Triage (the "Services") which may involve the observation or use of patients/patient records of hospitals, clinics or other health care organizations or entities that have entered into services agreements with Triage (these various health care groups shall be collectively referred to as the "Covered Entities"). In the course of providing such Services, Service Providers from time to time have access to or possession of Covered Entity's patient protected health information or "PHI," as such term is hereinafter defined. This Policy shall set forth the terms and conditions pursuant to which Service Providers shall use, secure and keep in confidence such PHI.

1. **Definitions**. For the purposes of this Policy, the following terms shall have the following meanings:

(a) **Electronic Protected Health Information or "EPHI"**. A subset of PHI, consisting of any PHI that is transmitted by electronic media or maintained in electronic media.

(b) **Individual**. The person who is the subject of the PHI, and has the same meaning as the term "individual" as defined by the HIPAA Regulations.

(c) **HIPAA Regulations**. Those regulations codified at Title 45 of the Code of Federal Regulations (C.F.R.) and relating to privacy and security of PHI.

(d) **Protected Health Information or "PHI"**. Any information concerning an Individual, whether oral or recorded in any form or medium: (1) that relates to the past, present or future physical or mental condition of such Individual; the provision of health care to such Individual; or the past, present or future payment for the provision of health care to such Individual; and (2) that identifies such Individual with respect to which there is a reasonable basis to believe the information can be used to identify such Individual, and shall have the meaning given to such term under the HIPAA Regulations.

2. **Disclosures and Use of PHI**. Subject to this Policy, Service Providers shall not the use the PHI except as necessary to provide the Services. Service Providers hereby agrees that the PHI provided or made available to it shall not be further used or disclosed other than as permitted or required by this Policy. Without limiting the foregoing, Service Providers agrees: (i) not to share PHI with anyone not directly involved in the patient's care or treatment; (ii) not to discuss PHI in areas where it may be overheard; (iii) not to access any PHI without specific direction by Triage; (iv) not to attempt access to PHI for personal reasons; (v) to inform Triage of any personal relationships which Service Providers may have with a patient or patient's family whose PHI Service Providers may access; (vi) if allowed access to EPHI by Triage or the Covered Entity, to clear computer screens of PHI before leaving the screen; (vii) to return any PHI provided on paper to the professional staff member or employee who provided it or to dispose of it within the facility using a shred-it box or as otherwise directed by the person who provided it; (viii) not to store or transmit any PHI using a portable device or any other electronic means; (ix) not to remove PHI in any form from the Covered Entity's facility; and (x) not to make any photographs, videos, voice recordings or any other reproduction of any PHI.

3. **Service Providers Obligations**.

(a) **Right of Access to PHI**. Service Providers and its representatives and employees shall forward all Individual requests for access to PHI to Triage within one (1) business days of receipt.

(b) **Amendment of PHI**. Service Providers shall forward all requests for amendments to an Individual's PHI to Triage within one (1) business days of receipt.

(c) **Accounting of Disclosures**. Service Providers shall forward all requests for an accounting of disclosures of PHI to Triage within one (1) business days of receipt.

(d) **Reports of Improper Use or Disclosure and Cooperation**. Service Providers shall report in writing to Triage within one (1) business day of discovery any use or disclosure of PHI not provided for or allowed by this Policy. Service Providers shall cooperate with Triage and the Covered Entity in any review/investigation of an actual or potential breach of HIPAA privacy or security regulations.

4. **Termination and Breach**.

(a) **Immediate Termination**. In regard to Triage employees, Triage reserves the rights to discipline any employee of Triage that has breached this Policy, including, the right to terminate such employee's employment with Triage. In regard to Triage subcontractors and agents, Triage reserves the right to terminate their agreement with such subcontractors and agents if they breach this Policy, and to seek such relief allowed by the contract with such subcontractor or agent and applicable law.

(b) **Injunctive Relief**. Notwithstanding any rights or remedies provided for in this Policy, Triage shall be entitled to obtain temporary and permanent injunctive relief from any court of competent jurisdiction to prevent or stop the unauthorized use or disclosure of PHI by Service Providers.

(c) **Return or Destruction of PHI**. Upon the termination or expiration of Service Providers' employment, agency or subcontract relationship with Triage, Service Providers hereby agrees to return to Triage all PHI received from, or created or received by Service Providers, from or on behalf of Covered Entity.

5. **General Provisions**.

(a) **State Law Preemption**. Certain provisions of state law relating to privacy of PHI may not be preempted by, and may supersede, the HIPAA Regulations. With respect to such provisions of state law not preempted by the HIPAA Regulations, Service Providers shall maintain full and complete compliance with all state privacy requirements.

(b) **Property Rights**. All PHI shall be and remain the property of Triage or the Covered Entity. Service Providers agrees that it shall not acquire any title or rights to any PHI.

(c) **Changes**. This Policy may be unilaterally modified by Triage in response to new statutory or regulatory requirements related to HIPAA, the HIPAA Regulations or other applicable state or federal law relating to security and privacy of PHI. Any ambiguity in the language contained in this Policy shall be interpreted consistent with HIPAA Regulations.

Agreed to and Acknowledged by:

By:_____

(Signature)

Name:_____

(Print or Type)

Company:_____

Date:_____