1 True Health, Inc.
HIPAA Compliance Statement

HIPAA Compliance as a "Covered Entity":

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") sets forth privacy and security standards for any organization (defined by HIPAA privacy rules as a "Covered Entity") that uses or discloses Protected Health Information (PHI). For information on HIPAA, please visit the U.S. Department of Health and Human Services website.

For a Covered Entity that treats patients/clients (or provides products and services to a Covered Entity who treat patients), HIPAA compliance is an organization-wide obligation requiring procedural standards and business practices that protect the privacy and security of patient/client information. As part of these obligations, the business must insure that it utilizes software with adequate safeguards to protect patient/client information.

1 True Health, Inc. ("1TH") has established detailed measures to ensure compliance with the regulations and conditions set forth in the Health Insurance Portability and Availability Act of 1996. 1TH is committed to continually improving our technology and service offerings to become increasingly more secure and better capable of meeting the high demand of information access against the increasing demands for information security. This statement will identify specific facets of our compliance with the HIPAA security standards and regulations.

Administrative Safeguards (HIPAA 164.308):
For administrative safeguard compliance, 1TH provides for the appropriate assignment of information and data access permissions to only the appropriate person(s). Actions are in place to govern the movement of our workforce and the privileges associated with those movements. 1TH has established internal guidelines and procedures to assure that no protected health information or personally-identifiable information is disclosed except to authorized parties. Information security awareness training is an annual mandated event for all staff, as well as annual review of contingency plans, audit trails, and security accreditation. Formal policies govern the conduct of employees regarding the confidentiality of patient/client information and specify penalties associated with breaches of such conduct.

Physical Safeguards (HIPAA 164.310):
With respect to physical safeguards compliance, 1TH and the data centers we utilize are physically secure. Access to all locations (down to the floor and room level) are all independently controlled via biometric or card access, preventing walk-up intrusion on a 24x7x365 basis. Our locations are monitored 24 hours a day with video surveillance, advanced fire protection systems, uninterruptible power, and emergency power for all systems. Annual reviews of the facility security plan, disaster recovery plan, and contingency plans are in place. Specific workstation usage and security measures are in place. Policies are also in place to guard against equipment disposal and reuse which may inadvertently compromise sensitive information.

Technical Safeguards (HIPAA 164.312):
1TH complies with technical safeguard regulations by enforcing unique user identifications, transaction logging and other audit controls, data integrity mechanisms, data encryption, verified backups, and entity authentication programs, including the expanding use of digital certificate technology for all staff, and increasing measures to provide complete data integrity.

HIPAA Compliance as a "Business Associate":

Under the HIPAA privacy rules 1TH is also considered a "Business Associate". This means that through contractual agreements with our customers (defined under HIPAA privacy rules as a "Covered Entity"), we give contractual guarantees that we will use Protected Health Information (PHI) and that we are granted access to PHI only for the purposes for which we have been contracted. We will safeguard the information from misuse, and will help the Covered Entity comply with their obligations under the HIPAA rules. If required by the Covered Entity, 1TH will make necessary changes to our contractual agreements to ensure our HIPAA compliance meets their specific needs.

We have taken the following steps to assure 1TH's HIPAA Compliance as a Business Associate:

Accounting of disclosures and audit trail issues:
We are appointed by and contracted to the Covered Entity to assist in claims management, billing, and payment/collection processes and are considered part of the Covered Entity's treatment, payment, and healthcare operations. A Covered Entity is not required by HIPAA regulations to keep an accounting of anyone within their own organization who has received (or had access to) medical information. Rather, the accounting provision only covers "disclosures," which are defined as the sharing of PHI with someone outside of an organization that is not a part of treatment, payment, or

healthcare operations (See Section 164.528(a) (right to accounting of disclosures) and Section 164.501 (definition of "disclosure") for additional information). The result of these exclusions are that a Covered Entity (and a Business Associate for a Covered Entity) is required to account for only a narrow category of disclosures that primarily are not related to healthcare, such as those made to law enforcement personnel or pursuant to a request for documents in a lawsuit.

Data is protected from unauthorized viewing/usage:
1TH's access to PHI is restricted via password to only those employees that are authorized to interact with PHI in the normal course of 1TH's deliverable products and services to the Covered Entity, and who have a need to know. Servers and data storage units are in a secured data center with limited access. Data is received and forwarded via automated, electronic processes where no direct human intervention is required. Access or viewing of PHI is only allowed when required to provide further support to the Covered Entity. Archive and backup tapes are encrypted and stored in a secured location.

Proper disposal of data:
As a service provider to a Covered Entity, we are required to securely retain and store PHI after the end of a Covered Entity's contractual agreement with 1TH for a timeframe established by applicable state and/or federal law. After that period, their data is deleted from the 1TH computer systems. No printed reports or paper copies are ever retained in our facility after the timeframe required by law. If reports are ever printed to further support the Covered Entity, they are shredded immediately upon completion of the task that required the paper output.

Privacy and Security Rule(s):
To protect the privacy and security of Protected Health Information we have implemented the following processes:

- Covered Entities must execute a Contractual Agreement to license our products and/or subscribe to our services
- All employees, contractors, sub-contractors, agents and representatives of 1TH are required to sign an agreement to abide by the HIPAA Privacy Act as well as a Confidentiality & Non-Disclosure agreement
- 1TH provides HIPAA and Security awareness training for all employees, contractors, sub-contractors, agents and representatives
- Employee termination security procedures have been defined and are used as needed
- 1TH utilizes the latest in information security technologies, including virus protection, internet firewalls, and SSL data transmission
- 1TH encrypts data stored in all storage locations and on all websites
- 1TH restricts access to PHI on a need to know basis (via passwords and by corporate policy)

- 1TH has implemented automatic password expiration for all users
- All 1TH locations are locked on a 24x7x365 based, requiring biometric or keycard access
- All 1TH locations have monitored security systems and video surveillance

1TH is committed to full and complete compliance with all HIPAA rules and regulations. If you would like additional information regarding our HIPAA compliance program, please contact us at info@1truehealthtech.com.