

**THINC, Inc.**  
**Privacy and Security Policy for**  
**Transactions that Require Consent**

**Table of Contents**

<b>Purpose</b> .....	1
I. <b>Consent</b> .....	2
II. <b>Authorization</b> .....	6
III. <b>Authentication</b> .....	8
IV. <b>Access</b> .....	9
V. <b>Audit</b> .....	12
VI. <b>Patient Engagement and Access</b> .....	15
VII. <b>Security Breach</b> .....	17
<b>Definitions</b> .....	19

**Purpose:**

THINC, through adoption of this policy by its Board of Directors, is committed to safeguarding the protected health information (PHI) of patients who consent to sharing their PHI with some or all of the participating provider organizations or other entities that access information through the THINC health information exchange.

THINC requires that all participating provider organizations or other entities that access PHI through the THINC health information exchange be in compliance with (i) current standards and requirements for safeguarding the privacy and security of PHI as set forth by THINC, (ii) the “RHIO Policies and Procedures” developed through the statewide collaboration process facilitated by the New York eHealth Collaborative and adopted by the NYS Department of Health (DOH) and (iii) any relevant New York State and federal laws and regulations.

Efforts to comply with this policy will involve not only THINC staff but also the participating organizations—hospitals, laboratories, physician practices, health centers, etc.—that participate in the THINC health information exchange.

## I. Consent

### A. Affirmative consent requirement.

1. Except as set forth in Section 2, below, THINC shall require its participants to obtain the patient's affirmative consent prior to accessing that patient's PHI via the THINC health information exchange.
2. THINC shall only allow "Level 1" uses of patient information via the THINC health information exchange. Level 1 uses are treatment, quality improvement, care management, and insurance coverage reviews.
3. THINC shall not permit "Level 2" uses of patient information via the THINC health information exchange. Level 2 uses are any uses of PHI other than Level 1 uses, including but not limited to payment, research and marketing.

### B. Exceptions to the affirmative consent requirement.

1. Affirmative patient consent is not required for one-to-one exchange of a patient's PHI. One-to-one exchange is a disclosure of PHI by one of the patient's providers to one or more providers treating the patient with the patient's knowledge and implicit or explicit consent. This one-to-one or point to point exchange is an electronic transfer of information that is understood and predictable to a patient, such as a referral to a specialist, a discharge summary sent to where the patient is transferred or discharged, or lab results sent to the practitioner who ordered them.

*a) Notwithstanding the exception for one-to-one exchange, participants still need to comply with existing state and Federal laws that already govern the disclosure of patient information, including those applicable to HIV/AIDS (NYS Public Health Law Article 27-F) and alcohol and substance abuse information (42 C.F.R. Part 2).*

2. Affirmative patient consent is not required for the purposes of public health reporting to a government agency when required or authorized by applicable State and federal laws and regulations.
3. Affirmative patient consent is not required for a break-the-glass scenario when treating a patient with an emergency condition if the following requirements are met:

*a) In the practitioner's judgment an emergency condition exists and the patient is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the patient's life or health;*

b) *The practitioner determines, in his or her reasonable judgment, that information that may be accessible via the THINC health information exchange may be material to emergency treatment;*

c) *No denial of consent to access the patient's information is currently in effect with respect to the participant organization with which the practitioner is affiliated;*

d) *The practitioner attests that all of the foregoing conditions have been satisfied, and the THINC health information exchange maintains a record of this access; and*

e) *THINC ensures that the break-the-glass access is terminated after the emergency treatment.*

4. Affirmative patient consent is not required for access of de-identified patient data for the following purposes: research approved by an Institutional Review Board or Privacy Board, public health purposes, or evaluation and improvement of THINC's operations.

a) *All other uses of de-identified data shall require affirmative consent.*

b) *THINC shall comply with and require its participants to comply with applicable standards for de-identification and re-identification of data, including those set forth in the HIPAA Privacy Rule at 45 C.F.R. § 164.514.*

C. Form of patient consent.

1. THINC shall require its participants to use the New York State Department of Health approved Level 1 consent form, unless THINC obtains approval from the New York State Department of Health to use an alternative form.

D. Sensitive health information.

1. Use of a Level 1 consent form authorizes a participant to access a patient's PHI, including sensitive health information. This information includes but is not limited to, HIV/AIDS, mental health, alcohol and substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information.

2. Participants must comply with applicable state and federal laws and regulations governing re-disclosure of sensitive health information, including those applicable to HIV/AIDS (NYS Public Health Law Article 27-F) and alcohol and substance abuse information (42 C.F.R. Part 2).

E. Special Provisions Relating to Minors

1. THINC and its participants may permit the exchange of information about minors age ten and below based on an affirmative consent executed by the minor's parent or legal guardian.
2. For exchanges of patient information that require patient consent, THINC and its participants may not exchange information about minors age eleven and above. In New York State, a minor may provide his or her own consent for certain types of health services without a parent's or guardian's permission (e.g., family planning, HIV testing, mental health or substance abuse treatment). Because it is difficult to reliably parse information related to health services provided pursuant to minor consent from other information about the minor, THINC and its participants cannot reasonably be sure whether the minor or the parent or guardian is the individual authorized to provide consent for exchange of PHI.
3. When a participant becomes aware that a minor is now emancipated, the participant must seek to obtain consent from that emancipated minor for transactions on the THINC exchange requiring consent. If a participant does not have knowledge that a minor is emancipated, the participant may rely on a consent previously granted by the parent or guardian.

F. Other Policies Related to Consent.

1. An affirmative consent obtained by a participant may apply to an affiliated practitioner of the participant.
2. An affirmative consent obtained by a participant shall permit authorized users of the participant to access the THINC health information exchange.
3. Electronic signatures may be used for the patient consent provided that the electronic signature meets the requirements of the federal E-SIGN statute, 15 U.S.C. § 7001 et seq., or any other applicable New York State or federal laws or regulations.
4. A patient shall be entitled to revoke his or her consent at any time. The patient should be informed, however, that a participant may have previously relied on the now-revoked consent to access a patient's PHI, and that PHI may continue to exist in and be retained in the record of that participant.
5. THINC shall provide and require its participants to provide patients with a list of or reference to all Data Suppliers to the THINC health information exchange at the time of the patient's consent. THINC shall maintain a current list of Data Suppliers and provide access to that list through its website.

6. All access to PHI via the THINC health information exchange shall be consistent with applicable federal, state and local laws and regulations. If applicable law requires that certain documentation exist or that other conditions be met prior to accessing PHI for a particular purpose, participants shall ensure that they have obtained the required documentation or met the requisite conditions.

7. THINC shall ensure that a payer organization does not access PHI through the health information exchange if a patient has requested, in accordance with the HIPAA Privacy Rule and HITECH, that the provider organization creating such information not disclose it to the payer organization.

8. All requests from government agencies for access to PHI for health oversight purposes, such as Medicaid audits, professional licensing reviews, and fraud and abuse investigations, shall be referred back to the participant organization from which the information originated.

## II. Authorization

- A. Authorized purposes for accessing the THINC health information exchange.
1. Individuals authorized to use the health information exchange shall only access PHI for the purposes of treatment, quality improvement, care management, public health reporting and administration of the exchange. Access for uses including research and payment will require a special, single use consent form from the individual patient as specified in THINC's *Consent Policy* and by the New York State Department of Health. (to be developed).
  2. For access to PHI for treatment, the individual and/or his or her organization must have a treatment relationship with the patient.
- B. Access Roles:
1. The THINC health information exchange shall employ role-based access as part of its security infrastructure and all users of the exchange will be assigned a defined access role.
  2. The access roles to which users of the THINC health information exchange can be assigned are:
    - a) *Practitioner with access to clinical information and Break the Glass authority;*
    - b) *Practitioner with access to clinical information but no Break the Glass authority;*
    - c) *Non-Practitioner, administrative staff with access to clinical information;*
    - d) *Non-Practitioner, administrative staff with access to non-clinical information;*
    - e) *RHIO administrators with access to non-clinical information; and*
    - f) *RHIO administrators with access to clinical information in order to engage in public health reporting purposes.*
- C. Process for Assignment:
1. THINC Process for Assignment.
    - a) *THINC's Executive Director shall assign THINC staff and the staff of its vendor their appropriate access roles taking into account each individual's job function and the information they need to successfully carry out that function.*

b) *The THINC Executive Director shall update access as needed to account for changes in personnel and job function and shall terminate accounts within 24 hours of termination of employment.*

2. Participant Organization System Administrator.

a) *Each participant organization shall designate a system administrator who is responsible for assigning its staff to appropriate access roles.*

b) *The participant organization shall inform THINC of the identity of the current system administrator and shall update THINC if the assignment of this role changes.*

3. Participant Organization Process for Assignment.

a) *When assigning staff of the participant organization into access roles, the system administrator shall take into account each individual's job function and the information needed to successfully carry out that job function.*

b) *The system administrator shall update access as needed to account for changes in personnel and job function and shall notify the THINC health information exchange to terminate accounts within 24 hours of termination of employment.*

c) *The participant organization shall be required to provide, on an annual basis, an updated list of its end-users to the THINC health information exchange and shall be able to respond to requests for information pursuant to an audit.*

### III. Authentication

#### A. Authentication of Identity of Authorized User Prior to Access

1. In instances in which an authorized user is attempting to access PHI through the health information exchange portal, THINC will authenticate the user's identity prior to providing the user with access to the exchange.

#### B. Authentication Requirements

##### 1. Current Required Authentication Standard

*a) Until such time as a determination is made by the New York State Department of Health (DOH) and/or federal statute or regulation that a higher standard is required, THINC shall authenticate each authorized user attempting to access the exchange through the portal through an authentication methodology that meets the minimum technical requirements for Authentication Assurance Level 2 (Level 2) set forth in the National Institute of Standards and Technology Special Publication 800-63 (NIST SP 800-63).*

*Level 2 requires, among other technical specifications, THINC or its participants to authenticate each authorized user's identity using only single-factor authentication, which queries authorized users for something they know (e.g. a password).*

##### 2. Anticipated Future Authentication Standard

*a) At such time as DOH and/or federal statute or regulation requires utilization of an authentication methodology that meets the minimum technical requirements for Authentication Assurance Level 3 (Level 3) as set forth in NIST SP 800-63, THINC will transition to Level 3 in conformity with the implementation approach and timeline articulated by DOH and/or federal requirements.*

*Level 3 will require, among other technical specifications, THINC or its participants to authenticate each authorized user's identity using multi-factor authentication. At this level, users will be queried for both something they know (e.g. a password) and something they have (e.g. cryptographic key or token). Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens, and "one-time passwords."*

#### C. Compliance with Policies Resulting from Statewide Risk Analysis

1. THINC shall comply with any changes in the Policies and Procedures developed via the Statewide Collaboration Process and amend its Policies and Procedures accordingly.

#### IV. Access

##### A. Access by User Name and Password

1. THINC shall require its participants to ensure that each authorized user is assigned a unique user name and password to provide such authorized user with access to patient information via the exchange.

THINC and its participants shall comply with the following standards:

a) *Authorized users shall be authenticated in accordance with the THINC Authentication Policy.*

b) *Passwords shall meet the password strength requirements set forth in NIST SP 800-63 This guideline does not set minimum password length and does not establish a requirement to change passwords frequently. Instead, a method is described for estimating the “guessing entropy” of passwords, based on the password rules (minimum length, types of characters required, randomly chosen or user chosen, and the use of dictionaries to rule out commonly chosen passwords). The method limits the maximum allowed probability (one chance in 16,384] that an attacker with no other knowledge of the password could guess the password over its entire life.*

c) *Group or temporary passwords shall be prohibited.*

d) *Authorized users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing passwords.*

e) *Authorized users shall be prohibited from sharing their user names and/or passwords with others and from using the user names and/or passwords of others.*

##### B. Authorized Purposes

1. THINC and its participants will permit authorized users to access PHI through the exchange only for purposes consistent with a patient’s affirmative consent.

##### C. Periods of Inactivity

1. THINC will ensure that an authorized user is automatically logged out of the exchange after a period of inactivity by such authorized user. The termination shall remain in effect until the authorized user reestablishes access using appropriate identification and authentication procedures. THINC shall establish the length of period of inactivity that will trigger such termination based on its internal risk analysis as well as organizational factors such as current technical infrastructure, hardware, and software security capabilities.

D. Failed Access Attempts

1. THINC shall enforce a limit of consecutive failed access attempts by an authorized user. Upon a fifth failed access attempt, THINC shall ensure that said authorized user's access to the exchange is disabled either by locking the account until release by a THINC administrator or by locking the account for a specific period of time as specified by THINC, after which the authorized user may reestablish access using appropriate identification and authentication procedures.

E. Access Limited to Minimum Necessary Information

1. THINC shall, and shall require its participants, to ensure that reasonable efforts are made, except in the case of access for treatment, to limit the information accessed through the exchange to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.

F. Record Locator Service and Other Comparable Directories

In operating a record locator service or other comparable directory, THINC shall, and shall require its participants, to:

1. Implement reasonable safeguards to minimize unauthorized incidental disclosures of PHI during the process of identifying a patient and locating a patient's medical records.

2. Prohibit authorized users from accessing PHI in any manner inconsistent with THINC's policies and procedures.

G. Training

The access controls set forth above will only be effective if 1) THINC's policies and procedures are clear; and 2) authorized users understand the policies and procedures and their responsibilities within them. As such, THINC shall develop and implement, either directly or through participants, minimum training requirements for educating individuals about the policies and procedures for accessing PHI via the exchange.

1. THINC shall, or shall require its participants to, provide either on-site training, web-based training, or comparable training tools so that authorized users are familiar with the operation of THINC and the policies and procedures governing access to information via the exchange.

2. THINC shall, or shall require its participants to, ensure that each authorized user undergoes such training prior to being granted access to information via the exchange.

3. THINC shall, or shall require its participants to, ensure that each authorized user signs a certification that he or she has received training and will comply with THINC's policies and procedures. Such certification shall be retained by THINC or its participants for at least six years.

4. THINC shall, or shall require its participants to, ensure that each authorized user undergo continuing and/or refresher training on a periodic basis as a condition of maintaining authorization to access patient information via the exchange.

H. Termination of Access and Other Sanctions

1. THINC shall ensure that access to the exchange of an authorized user or all of the participant's authorized users, if applicable, is terminated in the following situations and in accordance with the processes described:

*a) Immediately, or as promptly as reasonably practicable but in any event within one business day of termination of a participant's participation agreement with THINC; and/or*

*b) Immediately, or as promptly as reasonably practicable, but in any event within one business day of notification of termination of an authorized user's employment or affiliation with the participant.*

2. THINC shall require participants to notify THINC upon termination of an authorized user's employment or affiliation with the participant immediately or as promptly as reasonably practicable but in any event within one business day of termination.

3. THINC shall establish sanctions to redress policy or procedural violations. Sanctions could include temporary access prohibitions, re-training requirements, termination, or others processes THINC deems necessary in accordance with internal risk analyses.

## V. Audit

### A. Maintenance of Audit Logs

THINC shall maintain audit logs that document all access of PHI. These logs shall, at a minimum, include the following information:

1. The identity of the patient whose PHI was accessed;
2. The identity of the authorized user accessing the PHI;
3. The identity of the participant with which such authorized user is affiliated;
4. The type of transaction attempted (e.g. clinical summary exchange, public health reporting);
5. Whether or not the transaction was successful; and
6. In instances in which PHI was accessed through the portal, the audit log will also include any unsuccessful log-in attempts.

Audit logs shall be immutable and shall be maintained for a period of at least six years from the date on which the information was accessed.

### B. Periodic Audits

1. At a minimum, THINC shall audit, or require its participants to audit, the following:

*a) That affirmative consents are on file for patients whose PHI is accessed via the health information exchange, other than in Break the Glass situations;*

*b) That authorized users who access PHI via the health information exchange do so for authorized purposes; and*

*c) That applicable requirements were met where PHI was accessed through the Break the Glass function.*

2. THINC will conduct audits on at least an annual basis. THINC shall consider its own risk analyses and organizational factors, such as current technical infrastructure, hardware and software capabilities, to determine the reasonable and appropriate frequency with which to conduct audits more often than annually.

3. In performing annual audits, THINC will ensure that a representative sample of transactions is audited. The sample of transactions will also be reviewed to ensure that participants of varying transaction volume and organization type (e.g. hospitals, health centers, physician practices) are included.

4. If audits are conducted by participants rather than by THINC, THINC shall require each participant to conduct the audit and report its results within a reasonable time period. Results shall be reported in a format reasonably requested by THINC.

C. Participant Access to Audit Logs

1. THINC shall provide the participant, upon request, with the following information regarding any patient of the participant whose PHI was accessed via the health information exchange:

- a) *The name of each authorized user who accessed such patient's PHI in the prior 6-year period;*
- b) *The time and date of such access;*
- c) *The type of transaction attempted (e.g. clinical summary exchange, public health reporting); and*
- d) *Whether or not the transaction was successful.*

2. A participant shall only be entitled to receive audit log information listed above in instance in which either of the following conditions are satisfied:

- a) *The patient has provided affirmative consent for that participant to access his or her PHI; or*
- b) *The transaction(s) for which audit log information is sought originated from the requesting Participant. In this case, only the audit log information regarding transaction(s) originating from the requesting Participant shall be provided by THINC.*

D. Patient Access to Audit Information

1. THINC shall require its participants to provide patients, upon request, with the following information:

- a) *The name of each authorized user who accessed such patient's PHI in the prior 6-year period;*
- b) *The time and date of such access;*
- c) *The type of transaction attempted (e.g. clinical summary exchange, public health reporting); and*
- d) *Whether or not the transaction was successful.*

2. In response to a patient's request for information, THINC shall provide such information to participants within four calendar days and shall require participants to provide such information to patients as promptly as reasonably practicable but in no event no more than ten calendar days after the receipt of the request.

3. If requested, THINC shall, or shall require its participants to, provide such information to patients at no cost once in every 12-month period. THINC may establish a reasonable fee for any additional requests within a given 12-month period; provided that THINC shall waive any such fee where such additional request is based on reasonable suspicion of unauthorized access to the patient's PHI via the health information exchange.

4. THINC shall provide on its website notice of the availability of such information and information on how such information can be obtained.

E. Public Availability of Audits

1. THINC shall make the results of its periodic audit available on its website. The report of results shall include any major findings of the audit and steps taken by THINC to address these findings.

2. THINC shall not identify any individual recipients in the report of audit results available on the THINC website.

3. Audit results shall be made available as promptly as reasonably practicable, but in any event not more than 30 days after the completion of the audit.

## **VI. Patient Engagement and Access**

- A. Patient education regarding consent and how PHI may be shared.
  - 1. THINC must develop and/or approve a set of educational tools to help patients understand both the consent and the request process to allow their information to be transmitted for certain, approved uses through the THINC health information exchange.
  - 2. THINC must ensure that these educational tools are shared with the participating organizations and THINC must require participating organizations to share the education tools with their patients as needed to enable the consent process. THINC must also make the appropriate patient educational tools available on its website and by request.
  - 3. These educational tools must explain and meet the requirements set forth in THINC's Patient Consent Policy [to be developed].
- B. Patient access to personal health information.
  - 1. THINC will respond to patient inquiries regarding access in a quick and expeditious manner.
  - 2. At present, THINC shall not provide direct patient access to PHI via the exchange.
  - 3. Patients requesting access to their PHI will be directed by THINC to the appropriate contacts at the participant organization that generated the information.
  - 4. Participant organizations are required to have a policy addressing patient access and to educate and/or make available to the patient information about that access policy.
- C. List of data suppliers to the health information exchange.
  - 1. THINC shall maintain an updated list of organizations that supply patient data to the health information exchange. THINC shall make this list available on its website and upon request.
  - 2. THINC shall provide the participant organizations with an updated list of data suppliers. Participant organizations are required to provide this list to patients at the time of obtaining consent, consistent with THINC's Patient Consent Policy, or advise patients where the list may be obtained.
- D. THINC shall foster meaningful patient involvement in its governance and decision-making.
  - 1. THINC shall have at least one individual designated to represent the interests and views of patients as a full, voting member of its Board of Directors.

2. THINC shall ensure that its Patient and Consumer Committee has active patient involvement and that the decisions of this Committee take into careful account the views and interests of patients.
3. THINC shall post the minutes of the public session of all Board Meetings and committee meetings on its website to ensure transparency of operation and decision-making to the public.

## VII. Security Breach

### A. Notification and Remediation

When and if THINC becomes aware that a security breach has occurred or has reason to suspect that a security breach has occurred, it will:

1. Notify the patient(s) or require that the appropriate participant organization(s) notify the patient(s) about the breach of their unsecured PHI. Such notification shall be timely and be in writing. Those affected by the breach will be provided contact information for receiving more detailed information about the actual or suspected breach.
2. Notify or require that the appropriate participant organization(s) notify government agencies of the breach, or suspected breach, as required by Federal, state or local laws.
3. Notify the organization participating in the exchange if that organization's data was affected by the breach.
4. If the breach is the subject of a criminal investigation by law enforcement agency(s), these agencies have the right under law to require that notifications specified in items (1),(2) and (3) above be delayed.
5. Investigate the breach and/or require that the participating organization investigate the breach in the shortest time possible without reasonable delay. The purpose of the investigation is to determine the exact nature of the breach, the extent to which unsecured PHI has been compromised and to do a root cause analysis to identify its cause.
  - a) *If upon inquiry it is determined that the breach was unintentional and did not result in further disclosure of patient information beyond the authorized user, then THINC and the covered entity may reasonably determine that a breach did not occur.*
  - b) *THINC is responsible for the health information exchange and the actions of its own workforce. The participant organization is responsible for its own information systems and its own workforce. Once the site of breach has been determined, the responsible party must investigate and mitigate the breach per the requirements of this policy.*
  - c) *If a participant organization is unsure about whether something constitutes a breach, it should notify THINC and the two parties together will make a determination.*

6. Having identified the cause of the breach, THINC will develop or require that the appropriate participant organization(s) develop a remedial plan to prevent similar breaches from occurring in the future.

7. THINC and or the appropriate participant organization(s) will implement the remedial plans and work to reduce the harmful effects of the breach.

8. Require that when an organization participating in the exchange finds out that an actual or suspected breach may have occurred that they notify THINC in writing within 48 hours of their discovery.

**B. Enforcement and Sanction**

If a security breach is found to have been caused by or is believed to have been caused by an authorized user of the health information exchange, THINC will, where appropriate, apply sanctions to that authorized user and may also require its participants to apply sanctions to that user. The sanction(s) should be commensurate with the scope and impact of the breach, and may be, but not limited to, one or more of the following:

1. suspending or temporarily restricting the specific user's access to the health information exchange;
2. requiring the user to undergo additional training in the use of the health information exchange as a condition of removal of the suspension or restriction;
3. terminating access of the user to the health information exchange;
4. terminating a participant organization's access to the health information exchange;

If the participant organization applies the sanctions, a written report of the specific sanctions applied by the organization is required to be furnished to THINC within 24 hours of the effective date of the sanction(s).

## **Definitions**

The following definitions are derived from the *Privacy and Security Policies and Procedures for RHIOs and their Participants in New York State, Version 1.0* issued by the New York eHealth Collaborative.

***Affiliated Practitioner*** means (i) a practitioner employed by or under contract to a provider organization to render health care services to the Provider Organization's patients; (ii) a Practitioner on a Provider Organization's formal medical staff or (iii) a Practitioner providing services to a Provider Organization's patients pursuant to a cross-coverage or on-call arrangement.

***Breach*** means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the Protected Health Information. For purposes of this definition, "compromises the security or privacy of the Protected Health Information" means poses a significant risk of financial, reputational, or other harm to the individual. Breach excludes: (i) any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of a RHIO or Participant, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; (ii) any inadvertent disclosure by a person who is authorized to access Protected Health Information at a RHIO or Participant to another person authorized to access Protected Health Information at the same RHIO or Participant or organized health care arrangement in which a Participant participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or (iii) a disclosure of Protected Health Information where a RHIO or a Participant has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

***Break the Glass*** means the ability of an Authorized User to access a patient's Protected Health Information without obtaining an Affirmative Consent in accordance with the provisions of THINC Consent Policy (*to be developed*).

***Care Management*** means (i) assisting a patient in obtaining appropriate medical care, (ii) improving the quality of health care services provided to a patient, (iii) coordinating the provision of multiple health care services to a patient or (iv) supporting a patient in following a plan of medical care. Care Management does not include utilization review or other activities carried out by a payer organization to determine whether coverage should be extended or payment should be made for a health care service.

***Data Supplier*** means an individual or entity that supplies PHI to or through THINC's health information exchange. Data Suppliers include both Participants and entities that supply but do not access PHI through THINC's health information exchange (such as clinical laboratories and pharmacies).

**Emancipated Minor** means a minor who is emancipated on the basis of being married or in the armed services, or who is otherwise deemed emancipated under New York law.

**Insurance Coverage Review** means the use of information by a Participant (other than a Payer Organization) to determine which health plan covers the patient or the scope of the patient's health insurance benefits.

**Level 1 Uses** mean Treatment, Quality Improvement, Care Management, and Insurance Coverage Reviews.

**Level 2 Uses** mean any uses of PHI other than Level 1 Uses[, including but not limited to payment, research and marketing

**Marketing** has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH

**Minor Consent Information** means PHI relating to medical treatment of a minor for which the minor provided his or her own consent without a parent's or guardian's permission, as permitted by New York law for certain types of health services (e.g., reproductive health, HIV testing, mental health or substance abuse treatment) or services consented to by an emancipated minor.

**Practitioner** means a health care professional licensed under Title 8 of the New York Education Law or a resident or student acting under the supervision of such a professional. This Title includes, but is not limited to, physicians, nurses, pharmacists, physical therapists, midwifery, podiatry, optometry, social work, nutrition, mental health providers, and clinical laboratory personnel. A non-practitioner is an employee of a participant organization who is not a practitioner. A non-practitioner might include a medical assistant, a medical receptionist, a unit clerk or other administrative staff whose job function requires them to participate in the treatment relationship with the patient.

**Quality Improvement** means conducting quality measurement, assessment and improvement, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health and reducing health care costs, evaluating Practitioner and provider performance, clinical decision support tools, evidence-based clinical protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives and related functions. Care management by payers may include (i) assisting a patient in obtaining appropriate medical care, (ii) improving the quality of health care services provided to a patient, (iii) coordinating the provision of multiple health care services to a patient or (iv) supporting a patient in following a plan of medical care; provided, however, that no such activity may include utilization review or other tasks designed to determine whether a payer should cover or make payment for a health care service.

**Sensitive Health Information** means any information subject to special privacy protection under state or federal law, including but not limited to, HIV/AIDS, mental health, alcohol and

substance abuse, reproductive health, sexually-transmitted disease, and genetic testing information.

***Treatment*** means the provision, coordination, or management of health care and related services among health care providers or by a single health care provider, and may include providers sharing information with a third party. Consultation between health care providers regarding a patient and the referral of a patient from one health care provider to another also are included within the definition of Treatment.

***Unsecured Protected Health Information*** means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services in guidance issued under section 13402(h)(2) of HITECH.