Revised 12-09-2020

Propel Inc., HIPAA-Privacy Policy, The Complaint Process and Breach Notification

1.0 OBJECTIVE

Each Propel, Inc., ("Propel" or "Company") HIPAA related policy expressly adopts a continuing and overriding data security objective, which is to secure and keep private the protected health information (PHI) that the Company handles in conjunction with its clients, its clients' employees, its third-party data center host and other mission related third-party vendors, etc. For all other Propel® policies, information security sub-policies and protocols, this objective is also present as being implied and/or apparent when not expressly stated. Its underlying importance is such that it is made a part of every decision-making process within the Propel organization. An underlying piece of infrastructure supporting this objective is HIPAA's Privacy Rule, which requires Propel as a Business Associate to provide a clear policy to address health information privacy matters, specifically the process by which individuals can make complaints concerning privacy practices, policies and/or procedures. This policy provides the framework for handling Privacy Complaints consistent with HIPAA Privacy Rule requirements and includes Propel's responsibilities for notification in the event of a breach.

2.0 BACKGROUND AND PURPOSE

The Privacy Rule, a Federal law, gives individuals rights over their health information and sets rules and limits on who can look at and receive an individual's health information. See *Propel, Inc., HIPAA-Protected Health Information (PHI) Use and Disclosure Policy.* The Privacy Rule applies to all forms of individuals' PHI, whether electronic, written, or oral. The Security Rule, also a Federal law that protects health information in electronic form, requires entities covered by HIPAA to ensure that electronic protected health information is secure. See *Propel, Inc., HIPAA Workstation Security Policy; Propel, Inc., HIPAA-Security Rule Requirements-Administrative Safeguards Policy; Propel, Inc., HIPAA-Security Rule Requirements-Physical Safeguards Policy; and Propel, Inc., HIPAA-Security Rule Requirements-Technical Safeguards Policy.*

The Company is required by law to maintain the privacy and confidentiality of all PHI captured through the use of Propel technology. All authorized users (see Section 3.0 below) must protect the PHI provided to it, him or her, by employees of a Covered Entity as set forth in the relevant privacy provisions of HIPAA. Approved Propel team members may look at PHI only when there is an appropriate business reason to do so, such as to administer its products or services.

The purpose of this policy is to provide the framework/process for individuals to make complaints concerning Propel's privacy practices, and necessarily includes reciprocal procedures to govern Propel's response, as well as its responsibilities for notification in case of a breach.

3.0 SCOPE

This policy applies to all team members, contractors, vendors and agents (hereinafter referred to as "Authorized Users") with access privileges to Propel's networks. The policy's rules also apply to sending E-Mail and viewing intranet/internet web resources.

4.0 HIPAA RELATED DEFINITIONS (WITH COMMENTS AND PERTINENT HISTORY)

Term	Definition, Comments and Pertinent History
HIPAA 1996	The Health Insurance Portability and Accountability Act (HIPAA) of 1996 amended the Internal Revenue Service Code of 1986 to (among other things) improve portability and continuity of health insurance coverage, to combat waste, fraud, and abuse in

	health insurance and health care delivery and to simplify the administration of health insurance. HIPAA requires the Secretary of the U.S. Dept. of Health and Human Services (HHS) to develop regulations to protect the privacy and security of certain health information.
HIPAA Privacy Rule	This rule was established by the Secretary HHS to meet HIPAA requirements. Sometimes referred to as "Standards for Privacy of Individually Identifiable Health Information" (The Privacy Rule), it establishes national standards for the protection of protected health information (PHI).
HIPAA Security Rule	This rule was also established by the Secretary HHS to meet HIPAA requirements. Sometimes referred to as "Standards for the Protection of Electronic PHI (The Security Rule), it likewise establishes national standards for the protection of PHI, held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule and establishes the technical and non-technical safeguards that "covered entities" and "business associates" must put in place to protect electronic PHI. These include reasonable and appropriate administrative, technical and physical safeguards for protecting electronic PHI. The Security Rule also promotes two additional goals of maintaining the integrity and availability of electronic PHI. Under the Security Rule, "integrity" means that the electronic PHI is not altered or destroyed in an unauthorized manner. "Availability" means that the electronic PHI is accessible and usable on demand by an authorized user.
Covered Entity	It is defined by HIPAA as any health plan, healthcare clearinghouse or healthcare provider that transmits PHI in electronic form. For example, under Propel's business model, its clients are considered covered entities.
Business Associate	Likewise defined by HIPAA, it is an entity whose primary role is unrelated to PHI. Yet, the entity has authorized access to PHI in the provision of a service performed on behalf of a covered entity. Under Propel's business model, Propel is considered a business associate (BA) of each of its clients.
HITECH 2009	The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 was created as part of the American Recovery and Reinvestment Act (ARRA) of 2009. Among other things, HITECH gives the HHS Office of Civil Rights (OCR) enforcement powers for HIPAA matters.
Omnibus Final Rule 2013	This rule was created in 2013. It expanded and clarified the definition of BAs. Most importantly, the rule makes BAs directly accountable to the OCR for the protection of PHI.
HIPAA Regulation 164.310(c)	Final revision for this regulation came in March 2013. It requires both covered entities and business associates to implement physical safeguards for all workstations that access electronic PHI. It also requires that workstation access be restricted to authorized users.
Workstation(s)	It is defined as an electronic computing device, such as a laptop or desktop computer, or other device that performs a similar function, and includes electronic media stored in its immediate environment or on an accessible network server. Also covered are Personal Digital Assistant (PDA) devices and computer-based medical equipment containing or accessing patient information.
Workforce Member	Propel employee ("team member").
Physical Safeguards / HIPAA Regulation 164.310	Required by HIPAA's Security Rule, physical safeguards are physical measures, policies, and procedures designed to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and

	environmental hazards, and unauthorized intrusion. Workstation security, subsection (c) is one component of required physical safeguards.
Administrative Safeguards / HIPAA Regulation 164.308	Required by HIPAA's Security Rule, administrative safeguards are administrative actions, policies and procedures, designed to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI. These safeguards are also designed to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
Technical Safeguards / HIPAA Regulation 164.312	Required by HIPAA's Security Rule, technical safeguards are a combination of technology, policy and procedures which work synergistically to protect electronic PHI, as well as to control access to such information.
Risk Analysis / HIPAA Regulation 164.308 (a)(1)(ii)(A)	Referenced in HIPAA Regulations regarding Administrative Safeguards, this is a technique used to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic (PHI) held by covered entities and business associates. At Propel, this means to secure and keep private the PHI and PD that the Company handles in conjunction with its clients, its clients' employees, etc. It is a component of the risk management process and generally involves two (2) main parts: (1) to identify potential security risks (vulnerabilities and threats) and (2) to determine the probability of occurrence and magnitude of those risks. In Propel's technological environment, the most persistent and continuing risk threat is that of a data breach/unauthorized access to its electronic PHI. See Section 1.0 above (Objective). Also, in accordance with Section 8.0 of the *Propel, Inc., Information Security Management Policy (ISMP)*, the process of revision for any of Propel's compliance policies, information security sub-policies or HIPAA related policies also constitutes a "big picture" review of the Propel platform. This review also represents an exercise in continuing risk management as well as an ongoing data privacy impact assessment (DPIA) because each revision contains a review/consideration of at least the items listed in Section 8.0.
Risk Management / HIPAA Regulation 164.308(a)(1)(ii)(B)	Referenced in HIPAA Regulations regarding Administrative Safeguards, this process requires covered entities and business associates to implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA Regulation 164.306(a) Security Standards: General Rules.
Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI)	IIHI: A subset of health information that identifies the individual or can reasonably be used to identify the individual; HIPAA protects IIHI. Common individual identifiers include name, address, and social security number, but may also include date of birth, Zip Code, or county location. If the information is not individually identifiable, it is not protected by HIPAA. PHI: IIHI only becomes PHI when a Covered Entity or Business Associate creates, receives, stores, transmits or maintains the information (whether in electronic format or otherwise and includes paper and oral communication).
Use of PHI	This is the sharing, employment, application, utilization, examination or analysis of PHI within an entity that maintains/stores such PHI.
Disclosure of PHI	This is the release, transfer, provision of access to or divulging in any manner of such PHI outside the entity that maintains/stores such PHI.
Authorization	This is written permission to use and/or disclose an individual's PHI that contains the elements required by the Privacy Rule and is signed by such individual.

Data Aggregation	This is the process where raw data is gathered and expressed in a summary form for statistical analysis and the PHI is not individually identifiable (sometimes termed de-identified).
Breach	As defined in HIPAA Regulation 164.402, this means the acquisition, access, use, or disclosure of PHI in a manner not permitted, which compromises the security or privacy of the PHI. Three (3) regulatory exceptions exist: 1) unintentional acquisition, access or use of PHI by a team member if made in good faith and within the scope of authority, so long as it does not result in further prohibited use or disclosure; 2) inadvertent disclosure from one authorized person to another from the same entity where it is not further impermissibly used or disclosed; and 3) disclosure where the entity has a good faith belief that the unauthorized recipient would not reasonably have been able to retain the information.
Breach Notification Requirements Applicable to Business Associate	As defined in HIPAA Regulation 164.410(a)(1), following the discovery of a breach, Propel as a Business Associate is required to provide its client with a breach notification as described herein. Subsection (b) provides in part that the notification shall be made without unreasonable delay (usually within two (2) business days pursuant to the Business Associate Agreement (BAA) and in no case later than sixty (60) calendar days after discovery. Subsection (c)(1) requires that the notification shall include (to the extent possible) the identification of each individual whose unsecured PHI has been or is reasonably believed by the Business Associate to have been accessed, acquired, used or disclosed during the breach. Subsection (c)(2) requires Propel to provide its client with any other available information, that the client as Covered Entity is required to include in its notification to the individual under HIPAA Regulation 164.404(c). This provision requires Propel to provide such information at the time of Propel's notification of breach as referenced above. As a practical matter, this means that Propel's notification responsibilities run to its client as a Covered Entity, which in turn bears the responsibility for other required notification(s), which may include at least one of the following in addition to the affected individual(s): the Secretary HHS, the media and select states attorneys general. Simply stated, Propel has a duty (both under the applicable regulations and the terms of the BAA) to fully cooperate with the client's privacy official and to share the information and progress of its internal investigation. See Section 5.0 (below) for a description of the investigative process, etc.
Unsecured PHI	As defined in HIPAA Regulation 164.402, this means "PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons…" In a nutshell and for all practicable purposes, "unsecured PHI" essentially means "unencrypted" PHI. In the Propel business model, encryption of all PHI is an integral part of the Company's Information Security Management Program (ISMP). See *Propel, Inc., Information Security Sub-Policy Number 10-Encryption Key Management* and *Propel, Inc., Information Security Sub-Policy Number 5-Acceptable Encryption; Technologies in Use.*

5.0 PRIVACY COMPLAINTS and THE INVESTIGATION PROCESS / FILING A COMPLAINT WITH PROPEL / FILING A COMPLAINT WITH THE OFFICE OF CIVIL RIGHTS (OCR) / MISCELLANEOUS COMPLAINT RELATED ITEMS:

5.0 (a): Privacy Complaints and The Investigation Process: Any complaint regarding the use or disclosure of PHI is investigated and resolved in one of three (3) ways: internally within the Propel organization (this is rare because Propel almost never acts in a vacuum or unilaterally without its client), externally through the U. S. Department of Health and Human Services(HHS)-Office for Civil Rights-OCR, or as the preferred method, using a hybrid protocol whereby Propel's Chief Compliance Officer (CCO) conducts an investigation in close coordination with the client organization's designated privacy official. Propel as the Business Associate must promptly provide client as the Covered Entity with a detailed notification regarding any privacy complaint related situation. Unless the complaint is made directly to Propel, it is the client as Covered Entity, which bears the regulatory responsibility for specific HIPAA/HITECH/Omnibus Rule reporting/notification requirements to the complaining individual(s), other affected individuals, the media, the Secretary of HHS and perhaps, to one or more state government agencies. With the necessary investigative assistance and cooperation of Propel, as its Business Associate, the client as Covered Entity and Propel arrive at a set of findings, recommendation(s) for mitigation (if indicated by the findings) together with an agreed upon plan for final resolution.

Propel will launch its hybrid/collaborative effort as described above, when an offered complaint is received, or in the alternative, when notified by the client as Covered Entity, that it has received a complaint. Further, even if there has been no actual breach, nor have any individual rights been violated, nor was the complaint offered within 180 days of alleged violation, Propel® will nevertheless launch its investigation into the individual's concern for two (2) primary reasons. First, going through the investigative process reassures the complaining individual and further serves to create good will for the client organization. Secondly, the investigative process always brings a review of existing procedures, protocols and policies. Even if the alleged complaint is NOT found to reach the threshold of a real violation, nor has an actual breach occurred, Propel and/or its client may choose to take some action as a preventative measure. This concept is much the same as is provided for in *Propel, Inc., Platform Problem Management Policy and Procedures* which seeks to discover and fix the root causes of problems.

Upon receipt of a complaint, Propel's CCO will enter its details onto the Company's HIPAA Privacy Complaint Status and Notification Log and open a formal investigation. Among the CCO's first activities will be an effort to identify any policy violations and determine whether there has been a likely data breach impacting PHI. Additionally, the investigation seeks to discover any gaps and/or vulnerabilities which may be identified by interviews with the claimant or others, and the conduct of a risk assessment. Finding a likely data breach means that under present regulation, the breach is presumed, unless through a risk assessment, the CCO determines that there is a low probability that the data has been compromised (sometimes referred to as a "LoProCo"). Primary factors in this assessment process include the following: the nature and extent of the PHI; to whom the disclosure was made; whether the PHI was in fact acquired or viewed; whether the PHI was encrypted; and the potential risk of harm. The CCO will document investigative activities in the Company's HIPAA Privacy Complaint Status and Notification Log as the investigation proceeds. In accordance with the Business Associate Agreement, the client's privacy official will be notified within two (2) business days of Propel's discovery or receipt of the complaint.

5.0 (b): Filing A Complaint With Propel: Any Propel team member or employee of the client organization can file a privacy complaint using Propel technology:

1. **By telephone:** the individual can call the Company's corporate headquarters at +1 (615) 377-6116, state that he or she has a privacy complaint and ask for the Company's CCO;
2. **By E-mail:** the individual can submit a brief description of his/her privacy complaint to privacy@propelwellness.com. Such email will be promptly delivered to the Company's CCO;
3. **In person or by letter mailed to the Company's corporate office**: the individual can present a privacy complaint in person or via letter by visiting or mailing a letter to the Company's corporate offices:

Propel, Inc.
Attn: Chief Compliance Officer (CCO)
105 Continental Place
Suite 400
Brentwood, Tennessee 37027

5.0 (c): Filing A Complaint With OCR: An individual may file a health information privacy and security complaint with OCR, if he/she feels that Propel® has violated his/her (or someone else's) health information privacy rights, or has committed another violation of the Privacy, Security or Breach Notification Rules. OCR can be reached by calling (800) 368-1019. Note that a complaint may be filed with OCR at any time before, during or after initiating a complaint with Propel®.

5.0 (d): Miscellaneous Complaint Related Items:

- **CCO as Designated Privacy Official:** Propel's CCO serves as the Company's designated Privacy Official, as well as the Company's Data Protection Officer (DPO) as contemplated by the European Union's General Data Protection Regulation (GDPR). The CCO leads the Company's investigation relating to any health information privacy and security complaint.
- **No Retaliation or Waiver, Etc.:** It is the express policy of Propel® never to intimidate, threaten, coerce, discriminate against or take other retaliatory action against any team member or other individual, for his/her exercise of any right established by law or applicable regulation. This includes the filing, or support for the filing of a health information privacy and security complaint. Nor shall any team member or individual be required to execute a waiver of his/her rights as a condition precedent for any otherwise entitled benefit.
- **Company's Intention to Communicate:** It is the Company's policy that the CCO communicate as required by regulation, with individuals who have made health information privacy and security complaints directly to Propel. This communication seeks to ensure compliance with HIPAA Regulation 164.404 (Notification to Individuals), hereinafter referred to as "Regulation 164.404 Communication." Additionally, such communication serves to reiterate the Company's commitment to maintain objectivity in its investigation. Of course, when appropriate, the CCO's Regulation 164.404 Communication can be directed to an individual's personal representative or counsel. And, it is always the Company's intention to communicate in a timely, effective, sensitive and confidential manner. Propel will make all reasonable efforts to resolve and close complaints within thirty (30) business days of the opening of the investigation by the CCO.
- **CCO Reviews Findings, Etc., with Chief Administrative Officer (CAO); Seeks Concurrence:** To enhance the quality and thoroughness of the Company's investigative efforts, the CCO will open and share the investigative file, its findings, recommendations and conclusions with Propel's CAO. If the CCO and CAO concur regarding said findings, recommendations and conclusions, then the matter can be concluded and communicated as provided herein. If not, the CCO and CAO will promptly schedule a meeting with the Company's President and Chief Executive Officer (CEO), who (after allowing both the CCO and CAO to present their respective thoughts regarding proposed findings, recommendations and conclusions), will make a final determination regarding the situation.
- **Anonymous Complaints:** Anonymous complaints are accepted; however, insufficient information about relevant details may delay, hinder or prevent a more complete investigation.
- **Unexpected Investigative Delay:** At any time during the complaint process, if an unexpected investigative delay is experienced, complainant shall be made aware of the nature of the delay either by Propel or the client and provided a good faith time estimate regarding conclusion. The CCO will insert appropriate comments in the HIPAA Privacy Complaint Status and Notification Log.

- **Propel's HIPAA Privacy Complaint Status and Notification Log:** The CCO shall document all material, investigative activities in the HIPAA Privacy Complaint Status Log.
- **Cooperation with Client's Privacy Officer:** The CCO will cooperate with the client's privacy officer in all reasonable respects as he/she leads client's collateral investigation into the same set of facts (see Section (D)(18)(b)(4) of Propel's BAA template which provides as follows: "The Business Associate shall cooperate with Covered Entity in all reasonable respects so that Covered Entity and the Business Associate can ensure compliance with the breach notification provisions as set forth in the HITECH Act Breach Notification Rule (including providing background information regarding the Breach and its mitigation efforts following the Breach, and reviewing drafts of written notifications provided by the Covered Entity or the Business Associate)."

6.0 Training; Team Member Awareness:
All team members receive initial HIPAA training. Refresher training is also provided periodically, whenever job functions are affected by a material change in policies or procedures. Our HIPAA training seeks to emphasize how all of Propel's compliance policies, information security sub-policies, HIPAA related policies, etc., serve to enhance HIPAA Privacy and Security Rule requirements. This training is documented by "sign off" and retained for six years as required by HIPAA. See *Propel, Inc. Records Management, Document Retention and Disposal Policy*. Team members are reminded to remain continually aware/vigilant regarding the safety, security and sensitivity of all PHI and PD handled by the Company. (see Sections 3.12 and 3.13 of *Propel, Inc., Code of Conduct/Business Ethics Policy*). The Company trains on this premise, as well as on the accompanying requirement to follow defined procedures, all of which are designed to minimize the risk of data breach and/or unauthorized access. Such training includes the policies required by the Privacy and Security Rules (see Section 2.0 above), PHI use and disclosure, data privacy protection information, data security reminders, the process for protecting against malicious software, proper log-in procedures and procedures for creating, changing, and safeguarding passwords. Note that information security policies and sub-policies are in place for these and other training subjects. See *Propel, Inc., Information Security Sub-Policy Number 1-Privacy and GDPR Compliance; Propel, Inc., Information Security Sub-Policy Number 13-Cyber Security; Propel, Inc., Information Security Sub-Policy Number 4-Password Protection-User Responsibility Compliance.*

6.0 POLICY COMPLIANCE

6.1 Compliance Measurement: Propel's CCO in consultation with the Information Security Management Committee will verify compliance to this policy through various methods, which may include, but not be limited to one or more of the following: periodic internal and external technology audits, walk-throughs, video monitoring, business tool reports and inspection and/or log review. Feedback will be provided to the CAO, Information Security Management Committee and appropriate business unit manager(s).

6.2 Exceptions: Any exception to the policy must be approved by Propel's CAO and the Information Security Management Committee.

6.3 Non-Compliance: A team member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment for even the first offense.

7.0 RELATED STANDARDS, POLICIES AND PROCESSES
Please review the following related policies for details about The Privacy Rule, Privacy Complaints and Processes:

- *Propel, Inc., Code of Conduct/Business Ethics Policy*

- *Propel, Inc., HIPAA Workstation Security Policy*
- *Propel, Inc., HIPAA-Security Rule Requirements-Administrative Safeguards Policy*
- *Propel, Inc., HIPAA-Security Rule Requirements-Physical Safeguards Policy*
- *Propel, Inc., HIPAA-Security Rule Requirements-Technical Safeguards Policy*
- *Propel, Inc., HIPAA-Protected Health Information (PHI) Use and Disclosure Policy*
- *Propel, Inc., Information Security Sub-Policy Number 1-Privacy and GDPR Compliance*
- *Propel, Inc., Information Security Sub-Policy Number 4-Password Protection-User Responsibility*
- *Propel, Inc., Information Security Sub-Policy Number 5-Acceptable Encryption; Technologies in Use*
- *Propel, Inc., Information Security Sub-Policy Number 10-Encryption Key Management*
- *Propel, Inc., Information Security Sub-Policy Number 13-Cyber Security*
- *Propel, Inc., Platform Problem Management Policy and Procedures*
- *Propel, Inc., Propel, Inc. Records Management, Document Retention and Disposal Policy.*

Revision History: Date	**Revision No.**	**Description of Changes**
12-17-2017	01	Formalize HIPAA PHI Use and Disclosure Policy.
06-10-2019	02	This revision updates much of the original policy to incorporate related policies. This update also provided an opportunity to conduct a review of applicable HIPAA regulations and existing Propel procedures.
12-09-2020	3	This revision enhances the definition of Risk Analysis under Section 4.0, revises refresher training practice as provided in Section 6.0 and also provides housekeeping revisions commensurate with these updates. Data Privacy Impact Assessment (DPIA) conducted on Propel Platform.