Revised 12-09-2020

Propel Inc., HIPAA-Protected Health Information (PHI) Use and Disclosure Policy

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. At the center of this overriding data security objective lies protected health information (PHI), its use and disclosure. Here, beyond the above-referenced objective is a more focused imperative, which is simply to follow the rules governing the use and disclosure of PHI as set forth in HIPAA's Privacy Rule regulations (45 CFR Sections 164.502 through 164.514).

2.0 PURPOSE

The purpose of this policy is to explain how Propel uses and discloses PHI, how it strives to follow the rules by building them into the infrastructure of its key documents and finally, how following the rules serves to enhance the value of other Propel Information Security Policies and Sub-Policies. Of course, an important collateral purpose is to remind all team members that from a compliance perspective, "following the rules" is extremely important.

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 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).

5.0 GENERAL POLICY / REQUIRED DISCLOSURES / PERMITTED USES AND DISCLOSURES/ AUTHORIZED USES AND DISCLOSURES / LIMITING USES AND DISCLOSURES TO THE MINIMUM REQUIRED / DISCLOSURES TO OTHER BUSINESS ASSOCIATES:

5.0 (a): General Policy: Propel may not use or disclose PHI except as follows: (1) either as this policy permits or requires; or (2) as the individual who is the subject of the information formally authorizes.

5.0 (b): Required Disclosures: HIPAA requires the Company to disclose PHI in the following situations: (1) to individual employees of an associated Covered Entity specifically when such individuals request access to their own PHI or when they request an accounting of disclosures of their PHI; (2) To the Secretary of the United States (US) Department of Health and Human Services (HHS) when undertaking a compliance investigation, review or enforcement action; and (3) When otherwise required by law.

5.0 (c): Permitted Uses and Disclosures: HIPAA permits the Company to use and disclose PHI without an individual's written authorization for the following purposes or situations: (1) to the client's employee (individual); (2) As a part of an aggregated data set where the PHI is not individually identifiable; and (3) incidental to an otherwise permitted use and/or disclosure.

5.0 (d): Authorized Uses and Disclosures: The Company may use and disclose IIHI only with and employee's authorization for the following applicable purposes or situations: (1) for the client's (Covered Entity's) wellness program and (2) for any use or disclosure related to marketing in connection with the client's wellness program.

5.0 (e): Limiting Uses and Disclosures to the Minimum Necessary: Cognizant of the applicable regulatory requirements, Propel continually strives to use, disclose and request only the minimum amount of IIHI and PHI needed to accomplish the intended purpose of the use, disclosure or request for information except in the following circumstances: (1) disclosure to the employee who is the subject of the information; (2) use or disclosure made pursuant to an authorization; (3) disclosure to HHS for complaint investigation, compliance review or enforcement; (4) use or disclosure that is required by law; or (5) use or disclosure required for compliance with other HIPAA rules. Propel also makes "reasonable efforts" (as required by regulation) to comply with HIPAA's "Minimum Necessary" standard, by limiting team member access to IIHI and PHI. See Section 5.2 (e)(f)(g) of *Propel, Inc., HIPAA-Security Rule Requirements-Administrative Safeguards Policy*.

5.0 (f): Disclosures to Other Business Associates: The Company may disclose IIHI and PHI of client's employees to a Business Associate, as well as to appropriately and securely exchange such protected information, provided that such disclosure is permitted by the Covered Entity and is otherwise permitted by the HIPAA Privacy Rule. See also Section 5.2(a.) below regarding Propel's use of a "Mutual Nondisclosure and Confidentiality Agreement."

5.1 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.*

5.2 Key Documents and Infrastructure / Enhancing the Value of other Propel Information Security Policies and Sub-Policies:

a. **Business Associates Agreement / Mutual Nondisclosure and Confidentiality Agreement / Propel Recommended Terms of Use Policy and Consent:** In accordance with applicable provisions of HIPAA's Privacy Rule regulations (45 CFR Sections 164.502 through 164.514), Propel executes a "Business Associate Agreement" (BAA) with each of its Covered Entities (clients). While the precise language may vary slightly from client to client, the original template is maintained by Propel as a start point for each client relationship. In addition, when the client chooses to involve additional Business Associates in its wellness program, Propel executes a "Mutual Nondisclosure and Confidentiality Agreement" with each one. This document is likewise maintained by Propel as a start point and is sometimes customized by the client without sacrificing substantive features. Finally, as a requirement of the pre-launch activities relating to each client's program, Propel furnishes a recommended "Terms of Use Policy and Consent" template (likewise designed to comply with the applicable regulations). As discussed above, some clients use the template "as is" and others make entity specific changes. Note that Propel does not employ subcontractors as a part of its business model.

b. **Enhancing the Value of other Propel Information Security Policies and Sub-Policies:** The importance of proper use and disclosure of PHI cannot be overstated. See Section 1.0 above.

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 PHI, its use and disclosure:

- *Propel Code of Conduct/Business Ethics Policy*
- *Propel HIPAA Workstation Security Policy*
- *Propel HIPAA-Security Rule Requirements-Administrative Safeguards Policy*
- *Propel HIPAA-Security Rule Requirements-Physical Safeguards Policy*
- *Propel HIPAA-Security Rule Requirements-Technical Safeguards Policy*
- *Propel Information Security Sub-Policy Number 1-Privacy and GDPR Compliance*
- *Propel Information Security Sub-Policy Number 4-Password Protection-User Responsibility*
- *Propel information Security Sub-Policy Number 13-Cyber Security*

Revision History: Date	Revision No.	Description of Changes
12-17-2017	01	Formalize HIPAA PHI Use and Disclosure Policy.

05-20-2019	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 5.1 and also provides housekeeping revisions commensurate with these updates. Data Privacy Impact Assessment (DPIA) conducted on Propel Platform.