Revised 12-09-2020

Propel Inc., HIPAA-Security Rule Requirements-Administrative Safeguards 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. The Company's deployment of various administrative safeguards is an integral part of its effort to meet this objective.

2.0 PURPOSE

The purpose of this policy is to define the administrative safeguards (to include specific administrative security measures, policies and procedures) utilized by Propel® to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information (PHI) as well as to manage the conduct of team members relating to the protection of such information. Essentially, these administrative safeguards contemplate all administrative actions which Propel takes to ensure that the security measures (physical, workstation and technical) are managed properly, and further, how team members are trained, managed and held accountable for their role in protecting electronic PHI. See Section 4.0 HIPAA RELATED DEFINITIONS below. Because these safeguards are a required component of HIPAA's Security Rule Requirements which work in concert with one another, this policy incorporates by reference *Propel HIPAA Workstation Security Policy, Propel HIPAA Security Rule Requirements-Physical Safeguards Policy* and *Propel HIPAA Security Rule Requirements-Technical Safeguards Policy*. Propel continually strives to comply with the provisions of HIPAA, HITECH, the Final Omnibus Rule and specifically, HIPAA Regulation 164.308 (Administrative Safeguards).

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 POLICY

Propel's policy is designed to implement reasonable and appropriate administrative safeguards that establish the foundation for a HIPAA security program (See Section 5.2 below).

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 Reasonable and Appropriate Administrative Safeguards as Required by the HIPAA Security Rule:

a. **The Security Management Process (Risk Analysis and Risk Management):** This begins with the Company's adoption of a continuing and overriding data security objective, which is to secure and keep private the protected information that the Company handles, etc. (see Section 1.0 above). Also see Section 6.0 of *Propel's Information Security Management Policy* which provides in part, "The information security aspects of this work are classified as "Sub-Compliance Policies" for various information security subjects. Each of these sub-compliance policies is an exercise in continuing risk management." Propel focuses its attention upon HIPAA requirements, as well as upon achieving substantive compliance with the European Union's General Data Protection Regulation (GDPR). Indeed, each of the Company's security related policies and sub-policies periodically undergoes a thorough risk analysis and risk management review to confirm two (2) findings. First, that the Company is staying abreast of the ever-evolving vulnerabilities and threats, and second, that Propel's implemented countermeasures constitute reasonable and appropriate solutions to protect electronic PHI. This periodic review also prompts one (1) continuing question: Would the implementation of alternative countermeasures produce a "faster, better or smarter" means of addressing potential risks?

b. **Sanction Policy:** See Section 5.1 above (Training; Team Member Awareness) along with Section 6.3 below (Non-Compliance). Each team member's required HIPAA training includes an acknowledgement that he/she has read and understands the Company's HIPAA compliance policies, as well as the possible sanctions for violation thereof.

c. **Information System Activity Review:** Section 4.3 (Log Audit Frequency) of *Propel's Information Security Sub-Policy Number 11-Vulnerability Management and Penetration Testing* provides that it is the policy of the Company to manually review vulnerability scans and logs containing scan results on a periodic basis. In a recent review of this practice, the Chief Administrative Officer (CAO) Vice President-Application Architecture (VPAA) and Chief Compliance Officer (CCO) agreed that this practice should remain in place because the Company also receives a variety of automatic notifications (from automated scans and log reviews). Thus, a manual, periodic review of system activity complements the above referenced automatic

notifications. Further, Propel employs a formal logging or ticketing application for tracking database events. Examples of such formal logging or ticketing include documenting and tracking change control events, system development life cycle events and those associated with incident response.

d. Assigned Security Responsibility: The CCO serves as the Company's "Security Official" (the individual responsible for the development and implementation of the policies and procedures required by this subpart of the Security Rule). The CCO is also a member of the Information Security Management Committee and serves as Data Privacy Officer (DPO) for purposes of meeting GDPR requirements.

e. Team Member Security and Authorization Supervision: Each team member is granted only those data security access rights as may be reasonably necessary and appropriate to competently perform his/her assigned duties. The CAO manages this assignment process and meets with each new team member on his/her first day with the Company. Shortly thereafter, each new team member also participates in a personal interview with the CCO relative to compliance matters. Repeated attempts by any team member to access areas outside the scope of his/her granted access will be identified as such by the application architecture in place. The CAO is also advised of such attempts.

f. Function Specific Information Access Management: Group 1 (with the highest level of access) is comprised of team members working within the Information Technology (IT) function. It includes application architecture, back-end development and extends to the CAO who has overall responsibility for this group. Group 1 requires access to electronic PHI when required to program data feeds from clients or other business associates as well as to conduct detailed investigative analysis related to the Propel platform. Examples of data feeds include biometric screening data and eligibility files. Access may also be required when troubleshooting certain issues, or when the group may be required to perform other maintenance, modification or upgrade to the Propel technology and/or associated database structures. Group 2 (whose access is slightly reduced in scope) includes account management, client services and front-end development functions and extends to the Company's President and CEO. This group's access requirements are characterized by its need to troubleshoot certain individual-level issues and is normally limited to such electronic PHI entered in the client portal by each client's employees. Such data might include health check-in information, fitness entries or biometric screening information, but only to the extent that such information is the subject of or germane to a troubleshooting request. Group 3 has no access to electronic PHI. It includes sales and business development functions and extends to the Company's CCO as well.

g. Workforce Clearance Procedure: If a Group 3 team member requests clearance for temporary access, the Company's CAO will review the request, and consider alternative ways in which the need can be met. If in the sole discretion of the CAO, no reasonable alternative is available, the CAO is authorized to grant temporary, specific access for the limited purpose of the request and remove the authorization once the request is satisfied.

h. Termination Procedures: At the time of a team member's termination of employment (whether voluntary or otherwise), the CAO immediately orders that all network access be terminated. In addition, the former team member surrenders possession of any Company issued equipment to include hardware devices, building access cards and keys.

i. Security Incident Procedures, Response and Reporting: See *Propel's Information Security Sub-Policy Number 9-Intrusion Prevention and Platform Security Incident Response Procedures.*

j. **Contingency Plan and Data Back-Up Plan:** See Propel's Business Continuity Plan (BCP)-Disaster Recovery Plan.

k. **Business Associate Contracts and Other Arrangements:** Propel executes a Business Associate Agreement (BAA) with each of its Covered Entities (clients). While the precise language may vary 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 one or more Business Associates in the wellness program, Propel executes a Mutual Nondisclosure and Confidentiality Agreement with said Business Associate(s). This document is likewise maintained by Propel as a start point. Note that Propel does not employ subcontractors as a part of its business model.

l. **Evaluation:** At least annually (and more often if deemed necessary), the CCO will perform a technical and nontechnical evaluation of this policy and submit any revision(s) to the President and CEO for approval.

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 protecting all electronic PHI on the Propel platform:

- *Propel HIPAA Workstation Security Policy*
- *Propel HIPAA-Security Rule Requirements-Physical Safeguards Policy*
- *Propel HIPAA-Security Rule Requirements-Technical Safeguards Policy*
- *Propel Information Security Management Policy*
- *Propel Business Continuity Plan (BCP)-Disaster Recovery Plan*
- *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 9-Intrusion Prevention and Platform Security Incident Response Procedures*
- *Propel Information Security Sub-Policy Number 11-Vulnerability Management and Penetration Testing*
- *Propel information Security Sub-Policy Number 13-Cyber Security*

Revision History: Date	Revision No.	Description of Changes
12-17-2017	01	Formalize HIPAA Data Security-Administrative Safeguards Plan.
03-19-2019	02	This revision updates much of the original policy to incorporate related policies that also touch upon the security rule and technical safeguards. In addition, the update provides an opportunity to conduct a review of existing procedures.
03-27-2019	03	Policy undergoes title change: HIPAA-Security Rule Requirements-Administrative Safeguards Policy. Policy review along with a review of the applicable regulations. Section 5.2 has been reworked.
12-09-2020	04	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.