Revised 12-09-2020

Propel Inc., HIPAA-Security Rule Requirements-Physical Safeguards Policy

1.0 OBJECTIVE

Each Propel, Inc., ("Propel" or "Company") HIPAA related policy expressly adopts a continuing, overriding 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 physical safeguards is an integral part of its effort to meet this objective.

2.0 PURPOSE

The purpose of this policy is to define the physical safeguards (to include specific physical security measures, policies and procedures) utilized by Propel® to protect its electronic information systems, offices and equipment from natural and environmental hazards and unauthorized intrusion. Essentially, these physical security measures contemplate all means of physical access to electronic protected health information (PHI) and include security considerations relating to portable media, remote access, business continuity planning, restricted office access and pertinent maintenance records. See Section 4.0 HIPAA RELATED DEFINITIONS below. Because Propel's efforts relating to workstation security are a component of these physical safeguards, this policy incorporates by reference the *Propel, Inc., HIPAA Workstation Security Policy.* Generally, Propel continually strives to comply with the provisions of HIPAA, HITECH, the Final Omnibus Rule and specifically, HIPAA Regulation 164.310 (Physical 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.
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	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	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 for Authorized Users to take the following precautions (See Section 5.2 below) to secure and keep private the confidentiality, integrity and availability of sensitive information, including PHI and especially electronic PHI. Additionally, these precautions are designed to restrict access only to Authorized Users with the need to know/use the PHI.

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 Appropriate Precautions Include the following:

- Complying with provisions of *Propel HIPAA Workstation Security Policy;*
- Complying with provisions of *Propel Information Security Sub-Policy Number 4-Password Protection-User Responsibility Compliance;*
- Physically securing laptop computers at the end of normal working hours (even though each is considered as an endpoint device whose operating system uses full drive/disc encryption) by using cable locks or by placing laptops in locked drawers or cabinets. See Section 4.1 (Company Issued Laptop Computers-Full Drive/Disc Encryption) *Propel Information Security Sub Policy Number 10-Encryption Key Management;*
- If wireless network access is used, ensure access is secure by following the Company's wireless access procedures as described in *Propel Remote Technology Access Policy;*
- Complying with the Company's anti-virus policies (as described in *Propel Information Security Sub-Policy Number 13-Cyber Security);*
- *Complying with provisions of Propel Information Security Sub-Policy Number 6-Visitor Access and Control;*
- Physically securing entry to Propel's corporate offices with access control key cards/badges issued to all team members by the Chief Administrative Officer (CAO); the locked door entrance to the Company's offices provides barrier protection against unauthorized access and the key card/badge also serves as the only means by which to enter the building after normal business hours. Of course, key cards/badges carried by other tenants in the office building are not programmed to allow entry into Propel's offices;
- Within the Propel® offices, the corporate/office server and network hardware are secured in a separate locked and gated area. Keys are maintained by the CAO;
- Within the Propel Offices, team members know the value of limiting their access to the Company's WIFI for personal devices;
- Regarding Company issued laptop computers, any use of the computer's USB port for thumb drive (sometimes referred to as a pen drive, USB stick or flash drive) access/plug-in, should be done only with a thumb drive furnished by the Company;
- Complying with the *Propel Business Continuity Plan (BCP)-Disaster Recovery Plan* and *Propel Records Management, Document Retention and Disposal Policy,* especially regarding the integrity

and availability (see definitions above HIPAA Security Rule) of electronic PHI following a material business interruption;

- Ensuring that maintenance records are maintained for pertinent physical security and/or loss prevention repairs/upgrades; records are maintained by the CAO;
- At least annually, the Chief Compliance Officer (CCO) conducts a physical security review for the Company's offices, a material part of which is the CCO's loss prevention query to the building owner/property manager for information about criminal activity, attempts at unauthorized access, law enforcement contact information and any corrective action taken to include the installation camera systems, system upgrades and the like;
- Because more than 99% of PHI handled by Propel is done on the Propel platform, Propel's choice of IBM Corporation as the Company's third-party data center host stems in large part from the structural redundancies built into these data centers. See Section 5.0 (IBM CLOUD CERTIFICATIONS) contained within *Propel Information Security Sub-Policy Number 1-Privacy and GDPR Compliance*. In addition, the importance placed upon the physical security redundancies supporting each data center cannot be overstated. See Propel *Third-Party Due Diligence and Risk Management Policy.*
- Complying with provisions of *Propel Information Security Sub-Policy Number 2-Electronic/Media Sanitation, Disposal and Transfer Compliance*.

6.0 POLICY COMPLIANCE

6.1 Compliance Measurement: Propel's Chief Compliance Officer (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 Chief Administrative Officer (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 PHI on the Propel platform:

- *Propel HIPAA Workstation Security Policy*
- *Propel Code of Conduct-Business Ethics Policy*
- *Propel Acceptable Use Policy*
- *Propel Third-Party Due Diligence and Risk Management Policy*
- *Propel Information Security Sub-Policy Number 1-Privacy and GDPR Compliance*
- *Propel Information Security Sub-Policy Number 2-Electronic/Media Sanitation, Disposal and Transfer Compliance*
- *Propel Information Security Sub-Policy Number 4-Password Protection-User Responsibility Compliance*
- *Propel Information Security Sub-Policy Number 6-Visitor Access and Control*
- *Propel Information Security Sub-Policy Number 10- Encryption Key Management*

- *Propel Information Security Sub-Policy Number 13-Cyber Security*
- *Propel Remote Technology Access Policy*
- *Propel Business Continuity Plan (BCP)-Disaster Recovery Plan*
- *Propel Records Management, Document Retention and Disposal Policy*

Revision History: Date	**Revision No.**	**Description of Changes**
12-17-2017	01	Formalize HIPAA-Data Security Physical Safeguards Policy
03-11-2019	02	This revision updates much of the original policy to incorporate data security and privacy provisions contained within other corporate policies, information security sub-policies and procedures. Name change for policy: Propel, Inc., HIPAA-Security Rule Requirements-Technical Safeguards Policy.
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.