0760 NETWORK SECURITY POLICY
PRIVACY POLICIES
Collective Medical Technologies, Inc.

Objective

This Network Security Policy (this "Policy") applies to all Services provided by Collective Medical Technologies, Inc. ("Collective") pursuant to a Master Subscription Agreement or similar agreement (the "Underlying Agreement") between Collective and its customers (each referred to herein as the "Subscriber") and may be updated or amended by Collective from time to time in accordance with the terms of the Underlying Agreement. Collective and the Subscriber each acknowledge that the protection of the Services, the Subscriber's information systems, and the information transmitted and maintained via the Services requires coordination of certain security-related obligations between Collective and its Subscribers. This Policy applies to Collective's provision of the Services and to the Subscriber's use of the Services. Capitalized terms used but not defined in this Policy will have the meanings set out in the Underlying Agreement or in the Health Insurance Portability and Accountability Act of 1996, as amended from time to time, and its implementing regulations codified at 45 C.F.R. Parts 160 and 164 ("HIPAA").

Policy

1. Security of Services.

1.1. Business Associate Agreement. Collective shall comply with all information security obligations to which it is subject under the Business Associate Agreement between Collective and the Subscriber (the "BAA").

1.2. HIPAA Security Rule. Collective shall comply with, and if applicable obtain reasonable assurances that its subcontractors comply with, the HIPAA Security Rule with respect to the Services and any of the Subscriber's electronic Protected Health Information (PHI) that is maintained or transmitted through the Services or which Collective otherwise possesses or controls on the Subscriber's behalf.

1.3. Additional Safeguards. Collective may implement supplemental information-security safeguards which Collective deems appropriate, provided that such safeguards are no less stringent than those required by the BAA or HIPAA.

1.4. Subscriber Remedies. In the event that the Subscriber reasonably determines that Collective has materially failed to comply with this Section 1 and that such failure creates a material vulnerability affecting the Subscriber's information systems, the Subscriber shall promptly notify Collective of such determination and may suspend or limit access by the Services to the Subscriber's information systems. Such a failure by Collective shall be deemed a curable breach of the Underlying Agreement, provided that upon receipt of notice from the Subscriber of such a breach, Collective shall use its best efforts to come into compliance with this Section 1 within the applicable cure period(s) set forth in the Underlying Agreement. Upon Collective's demonstration to the Subscriber that Collective is in compliance with this Section 1, the Subscriber shall resume its regular connection to the Services. In the event of Collective's continuing, uncured failure to comply with this Section 1, the Subscriber may proceed to terminate the Underlying Agreement as provided therein. The Subscriber shall not be liable for any subscription fees

otherwise payable to Collective for Services during any period during which the Services are fully suspended under this Section 1.

2. Subscriber Security Administration.

2.1. HIPAA Security Rule. The Subscriber shall at all times comply with the HIPAA Security Rule in managing and administering its Users' access to and use of the Services and the information obtained therefrom. The Subscriber specifically represents that it complies with the following practices:

2.1.1. *User Clearance*. The Subscriber maintains policies and procedures providing for reasonable and appropriate determination of the access privileges of its Users.

2.1.2. *User Authorization*. The Subscriber maintains policies and procedures for authorizing, suspending, and terminating the authorization of its Users to access the Services or otherwise obtain or disclose information through the Services.

2.1.3. *User Access Limitations*. The Subscriber maintains policies and procedures requiring its Users to limit their access to and use of the Services and information available through the Services in accordance with HIPAA's minimum-necessary standard and all other applicable federal and state laws.

2.1.4. *Acceptable Use Management*. The Subscriber maintains and enforces appropriate acceptable-use policies in connection with all information systems, workstations, and devices whereby its Users access the Services or any data from the Services.

2.1.5. *Access Controls*. The Subscriber maintains appropriate administrative, physical, and technical access control safeguards in accordance with the HIPAA Security Rule designed to prevent non-Users from accessing the Services or any information from the Services and to detect and respond to any such unauthorized activity.

2.1.6. *Workstation and Device Management*. The Subscriber maintains policies and procedures for the authorization and secure operation and disposal of all of its devices which the Subscriber permits its Users to use in order to access the Services (each an "Authorized Device"). Collective may, in its discretion, limit or prohibit the use of certain devices as Authorized Devices upon notice to the Subscriber of such limitation or prohibition or by an update to the Minimum System Requirements.

2.1.7. *User Training*. The Subscriber conducts, and requires all Users to undergo, privacy and security training in accordance with the requirements of applicable federal and state laws, the Underlying Agreement, any applicable Business Associate Agreement, this Policy, and the Terms of Use.

2.1.8. *Sanctions for Violations*. The Subscriber conducts sanctions and disciplinary procedures for Users and any other person subject to the Subscriber's authority, for accessing or using the Services in violation of applicable federal or state laws, the Underlying Agreement, any applicable Business Associate Agreement, this Policy, or any other Network Policy, or the Subscriber's own policies related to information privacy and security.

2.1.9. *Audit Trails*. The Subscriber maintains audit logs for its transmissions of PHI to or from the Services.

2.1.10. *Software Management*. The Subscriber maintains and enforces policies and procedures related to patch management and change management for hardware and software included in the Subscriber's information systems which access, or which may be used to access, the Services or any information from the Services.

2.1.11. *Malware Protection*. The Subscriber maintains up-to-date anti-virus and anti-malware software on all applicable components of the Subscriber's information systems which access, or which may be used to access, the Services or any information from the Services.

2.1.12. *Other Safeguards*. The Subscriber will employ other reasonable safeguards identified by Collective to the extent that Collective determines such additional safeguards to be reasonably necessary to protect the Services or the information from the Services.

2.2. Collective Remedies. In the event that Collective determines that a failure by the Subscriber to comply with this Section 2 creates a material vulnerability potentially affecting the confidentiality, integrity, or availability of (i) the Services, (ii) Collective's or its Subscribers' information systems, or (iii) any PHI or related information, Collective shall promptly notify the Subscriber of such determination and may, at Collective's reasonable discretion, suspend or limit access to and/or use of the Services by some or all of the Subscriber's Users, and/or to or from the Subscriber's information systems and/or Authorized Devices. Such a failure by the Subscriber shall be deemed a curable breach of the Underlying Agreement, provided that upon the Subscriber's receipt of notice from Collective of such a breach the Subscriber shall use its best efforts to come into compliance with this Section 2 within the applicable cure period(s) set forth in the Underlying Agreement. Upon the Subscriber's demonstration that it is in compliance with this Section 2 to Collective's reasonable satisfaction, Collective shall discontinue the Subscriber's suspension from or limitation to the applicable Services. In the event of the Subscriber's continuing, uncured failure to comply with this Section 2, Collective may proceed to terminate the Underlying Agreement as provided therein. The Subscriber shall continue to be liable for any applicable subscription fees otherwise payable to Collective by the Subscriber for any period during which the Services are limited or suspended due to the Subscriber's failure under this Section 2.

3. Security Incidents and Breaches.

3.1. Definitions. The following definitions shall apply for purposes of this Policy.

3.1.1. *"Access Attempts"* means unauthorized probes, scans, "pings," and other activities which may or may not indicate threats, whose sources may be difficult or impossible to identify, whose motives are generally unknown, and which do not result in access to the Services, the Subscriber's information systems, or to Unsecured Protected Health Information.

3.1.2. *"Breach"* means a Breach of Unsecured Protected Health Information as defined in 45 CFR § 164.402 as well as any Unauthorized Use or Disclosure of PHI or related information to the extent that applicable state law requires such Unauthorized Use or Disclosure to be reported to a state agency or disclosed to the individuals who are the subject of such information.

3.1.3. *"Security Incident"* has the definition set forth at 45 CFR § 164.304 with respect to the Services and to the Subscriber's information systems, but for purposes of this Policy does not include an Access Attempt.

3.1.4. *"Unauthorized Use or Disclosure"* means any access, use, or disclosure of PHI that is not permitted under the Underlying Agreement, the BAA, this Policy, or any other Network Policy.

3.2. Monitoring.

3.2.1. *Services Monitoring*. Collective is responsible for monitoring or for ensuring the monitoring of all activity in (i) the Services, (ii) any information system that Collective uses to host, operate, or manage the Services, and (iii) any facilities where Collective or its subcontractors host, operate, or manage the Services.

3.2.2. *Subscriber Monitoring*. The Subscriber is responsible for monitoring or for ensuring the monitoring of all activity on its information systems, workstations, Authorized Devices, and facilities where it accesses the Services or any data from the Services.

3.3. Investigations.

3.3.1. *Collective Investigations*. Collective shall investigate any Unauthorized Use or Disclosure of the Subscriber's PHI and any Security Incident which may affect or have affected the Services or any of Subscriber's PHI promptly upon receiving notice from the Subscriber or otherwise becoming aware of such an event. Collective shall document the results of each such investigation.

3.3.2. *Subscriber Investigations*. The Subscriber shall investigate any Unauthorized Use or Disclosure of Collective-sourced PHI and any Security Incident which may affect or have affected the Services or any PHI therefrom promptly upon receiving notice from Collective or otherwise becoming aware of such an event. The Subscriber shall document the results of each such investigation.

3.3.3. *Breach Determination*. If Collective determines that an Unauthorized Disclosure of PHI constitutes a Breach, Collective shall promptly notify the Subscriber of this determination; provided, however, that the Covered Entity whose PHI is affected by the Unauthorized Use or Disclosure, or that Covered Entity's designee if applicable, shall be responsible for making its own determination of whether an event constitutes a Breach. Furthermore, any other affected party may also make such a determination, at its discretion.

3.3.4. *Cooperation*. Collective and the Subscriber shall reasonably cooperate with one another in their performance of the investigations and determinations described in this Section and in identifying and implementing measures to mitigate the harmful effects of any event and to prevent events of the same type to the extent practicable.

3.4. Reporting and Notifications.

3.4.1. *Notice of ongoing Access Attempts*. Collective and the Subscriber acknowledge and agree that Access Attempts fall under HIPAA's definition of a Security Event but that Collective's ongoing reporting and the Subscriber's review of information about Access Attempts would be materially burdensome to both parties without reducing risks to Information Systems or Protected Health Information. Therefore, provided that Collective ensures that there is appropriate review of logs and other records of Access Attempts, and investigates events where it is not clear whether or not an apparent Access Attempt was successful, this provision shall serve as Collective's notice to the Subscriber that Access Attempts occur and are anticipated to continue occurring with respect to the systems providing the Services. By using the Services, the Subscriber acknowledges this notification,

and that Collective shall not be required to provide further notification of Access Attempts except to the extent that they otherwise constitute Security Incidents as defined in this Policy.

3.4.2. *Collective Reporting to the Subscriber*. Collective shall require its employees and any applicable subcontractors to report to Collective any Security Incident (not including Access Attempts) and Unauthorized Uses or Disclosures of PHI of which they become aware. Collective shall report to the Subscriber any Security Incident (not including Access Attempts) or Breach which affects Subscriber's PHI within ten (10) business days of Collective's determination thereof or within the time period(s) set forth in the BAA, whichever is shorter.

3.4.3. *Subscriber Reporting to Collective*. The Subscriber shall require its Users to report to the Subscriber any Security Incident (not including Access Attempts) and Unauthorized Uses or Disclosures of PHI of which they become aware. The Subscriber shall report to Collective any Security Incident (not including Access Attempts) or Breach involving the Services or Collective-sourced PHI within ten (10) business days of the Subscriber's determination thereof.

3.4.4. *Breach Notifications*. Collective and the Subscriber each acknowledge and agree that, as between Collective and the Subscriber, the Subscriber has the more direct provider-patient, plan-member, or entity-customer relationship with the individuals who are the subject of the PHI used and disclosed via the Services. Accordingly, the Subscriber shall be responsible for providing notification of Breaches to the affected individuals, applicable regulatory authorities, and the media where required by law or elected by the Subscriber. Any notification by the Subscriber to affected individuals, regulatory authorities, or media shall be deemed notification as well by Collective and its subcontractors, if applicable, and the Subscriber shall identify Collective as a notifying party in the notification, except to the extent that Collective directs otherwise in writing. In the event that the Subscriber elects not to or fails to timely notify potentially affected individuals, regulatory authorities, or media as provided above, and Collective reasonably determines that it may be required by law to give such notification, Collective may give such notification at its discretion.

3.4.5. *Other Law Enforcement Notification*. For the avoidance of doubt, a Party may notify appropriate law enforcement agencies in the event that it reasonably believes that an Unauthorized Use or Disclosure of PHI is the result of criminal activity.

[Remainder of page intentionally blank.]