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

Objective

This Security Policy ("Policy") applies to all Services provided by Collective Medical Technologies, Inc. ("CMT") pursuant to a Master Subscription Agreement ("Underlying Agreement") and may be updated or amended by CMT from time to time at CMT's sole discretion.

A. CMT administers the Services to support the exchange of information among health care organizations who have entered into the Underlying Agreement ("Subscribers"). The Subscriber is a health care organization which has entered into the Underlying Agreement and uses the Services.

B. Protection of the Services, as well as the Information Systems of Subscribers and the information transmitted and maintained using the Services requires coordination and an allocation of security-related obligations among CMT and its Subscribers. This Policy therefore applies to the use of the Services by CMT and all Subscribers.

Policy

1. Security of Services.

CMT shall comply with, and if applicable obtain reasonable assurances that Subcontractors comply with, the Security Rule with respect to the Services and any electronic Protected Health Information maintained or stored or in transmission through the Services, or otherwise in the possession or control of CMT or any Subcontractor for purposes of the Underlying Agreement, provided that CMT may implement supplemental or more stringent safeguards which CMT deems appropriate.

2. Subscriber Security Administration.

The Subscriber shall comply with the Security Rule in managing and administering access to and use of the Services from its Facilities or otherwise using its Information Systems or Authorized Devices, including but not limited to the following:

2.1. User Clearance. Policies and procedures providing for reasonable and appropriate determination of the access privileges of Users.

2.2. User Authorization. Policies and procedures for authorizing, suspending and terminating the authorization of its Users who are authorized to access and use any of the Services and obtain or disclose information through the Services on behalf of the Subscriber.

2.3. User Access Limitations. Policies and procedures requiring Users to limit their access to and use of the Services and information available through the Services to the minimum necessary (except for Treatment purposes), and consistent with applicable federal and state law.

2.4. Acceptable Use Management. Acceptable use management services for the Subscriber's Information System(s) and Workstations by any User of the Subscriber's Information System(s) or Workstations.

2.5. Access Controls. Administrative, physical and technical access control Safeguards to prevent parties not authorized as Users by the Subscriber from using the Subscriber's Information System(s) to seek or obtain access to any of the Services, information available through the Services, or any other Information System, and to detect and respond to any such unauthorized activity.

2.6. Workstation and Device Management. Policies and procedures for the authorization and secure operation and disposal of all Authorized Devices which the Subscriber permits its Users to use in order to access the Services. CMT may limit or prohibit the use of certain types of device as Authorized Devices, for example smartphones, if their security has not been demonstrated to CMT's satisfaction in its sole discretion.

2.7. User Training. Appropriate and adequate training to all Users in the requirements of applicable federal and state laws, the Underlying Agreement, any applicable Business Associate Agreement, this Policy and the Terms of Use.

2.8. Sanctions for Violations. Sanctions and disciplinary procedures for the Subscriber's Users and other members of the Subscriber's Workforce 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, the Sensitive Information Policy, the Terms of Use, or the Subscriber's policies, procedures or technical controls implemented for purposes of access to and use of the Services.

2.9. Audit Trails. Audit logs for transactions in which any Protected Information is transmitted to or from the Services and the Subscriber's Information System(s) or Authorized Devices.

2.10. Software Management. Patch management, change management and updating policies and procedures for hardware and software included in the Subscriber's Information System(s) and Authorized Devices which may be used to access the Services.

2.11. Malware Protection. Anti-virus and other anti-malware software or other applications intended to identify, prevent the download of, disable, uninstall or otherwise affect any computer virus, worm, "Trojan horse," spyware, or other potentially harmful software in or accessing Subscriber's Information System(s) or Authorized Devices, and/or using them to access the Services, or the Information System of any party.

2.12. Any other Safeguard CMT has determined is Reasonable and Appropriate to protect (i) the Services, (ii) the Information System or Authorized Devices of any party, or (iii) any information, including but not limited to Protected Health Information.

3. Security Incidents and Breaches. CMT, all Subscribers and all Users shall comply with the following Security Incident and Breach Response Policies:

3.1. Definitions. The following definitions shall apply for purposes of this Section 3.

3.1.1. *Access Attempts*. Information Systems are the frequent target of probes, scans, "pings" and other activities which may or may not indicate threats, whose sources may be difficult or impossible to identify and whose motives are unknown, and which do not result in access to any Information System or Protected Health Information ("Access Attempts").

3.1.2. *Security Incidents*. A "Security Incident" is defined under the Security Rule as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of electronic Protected Health Information or interference with the system operations of the Services, but for purposes of this Policy does not include an Access Attempt.

3.1.3. *Unauthorized Use or Disclosure*. An Unauthorized Use or Disclosure is any Access, Use or Disclosure of Protected Health Information which is not permitted under the Underlying Agreement, any applicable Business Associate Agreement, this Policy or the Terms of Use.

3.1.4. *Breach*. A Breach is:

3.1.4.1. Any acquisition, Access, Use or Disclosure of Protected Health Information in a manner not permitted under the Privacy Rule which compromises the security or privacy of Protected Health Information.

3.1.4.2. For purposes of this definition, "compromises the security or privacy of the Protected Health Information" means that the event poses more than a low probability of financial, reputational, or other harm to the Individual, but does not include a use or disclosure of Protected Health Information if:

3.1.4.2.1. The information does not include the identifiers listed at 45 CFR § 164.514(e)(2), and CMT does not have actual knowledge that the information could be used alone or in combination with other information to identify an Individual who is the subject of the information;

3.1.4.2.2. The event was an unintentional acquisition, Access, or Use of the Protected Health Information by a workforce member or person acting under the authority of a Covered Entity or a Business Associate which was made in good faith and within the scope of authority and did not result in further Use or Disclosure in a manner not permitted under the Privacy Rule;

3.1.4.2.3. An inadvertent Disclosure by a person authorized to Access the Protected Health Information at a Covered Entity or Business Associate to another person authorized to Access the Protected Health Information at the same Covered Entity or Business Associate, or Organized Health Care Arrangement in which the Covered Entity participates, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under the Privacy Rule; and

3.1.4.2.4. A Disclosure of Protected Health Information where the Subscriber or CMT, whichever is responsible for investigation of the Disclosure under Section 3.3 of this Policy, following such investigation has a good faith belief that an unauthorized person to

whom the Disclosure was made would not reasonably have been able to retain such information.

3.1.4.3. The unauthorized acquisition of personally identifiable information, as defined under the laws of the State of the Individual's residence, which triggers an obligation to notify affected Individuals and/or State agencies.

3.2. Monitoring

3.2.1. *Services Monitoring*. CMT shall be responsible for monitoring or providing for the monitoring of all activity in the Services, and in any Information System used to host, operate or manage Services, and at Facilities where equipment used to host, operate or manage the Services is located.

3.2.2. *Subscriber Monitoring*. Each Subscriber shall be responsible for monitoring activity on its Information System(s), on its Workstations and other Authorized Devices, and at its Facilities.

3.2.3. *Reporting of Security Incidents and Unauthorized Use or Disclosure*.

3.2.3.1. *Notification of Access Attempts*. Access Attempts are recorded in various system logs, and fall under the definition of "Security Incident" in the Security Rule. Because Access Attempts fall under the definition of Security Incident CMT is required to report them to Subscribers. At the same time CMT's 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.

3.2.3.2. Therefore, provided that CMT 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 CMT'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 CMT shall not be required to provide further notification of Access Attempts unless they constitute Security Incidents.

3.2.4. *CMT Reporting*. CMT shall report to the Subscriber any Security Incident or Unauthorized Use or Disclosure of Protected Health Information which it determines has occurred which affects, or may affect, Protected Health Information of the Subscriber within one (1) business day of such determination.

3.2.5. *Subscriber Reporting*. Each Subscriber shall report to CMT any Security Incident (not including Access Attempts) or Unauthorized Use or Disclosure of Protected Health Information of which it becomes aware, which may affect or involve the use or access to Services.

3.2.6. *User Reporting*. All Users shall report to their Subscriber any Security Incident (not including Access Attempts, unless required by Subscriber policy) or Unauthorized Use or Disclosure incidents of Protected Health Information which they become aware, which may affect or involve the use or access to Services.

3.2.7. *Security Incident and Unauthorized Use or Disclosure Investigation*.

3.2.7.1. *CMT Investigation*. CMT shall investigate any Unauthorized Use or Disclosure and any Security Incident which may affect or have affected Services or any Information System used to host, operate or manage Services or any Protected Health Information maintained, stored or in transmission or processing in Services, promptly upon receiving notice from a Subscriber or other information which reasonably indicates the potential occurrence of a such an event. CMT shall document the results of each such investigation. CMT shall provide for reasonable periodic reporting of Security Incidents and Unauthorized Uses or Disclosures which do not meet the definition of "Breach" in Subsection 3.1(d) to the Subscriber, and shall promptly report any Security Incident or Unauthorized Use or Disclosure to Subscriber which presents or indicates a potentially material threat to the Subscriber's Protected Health Information, Information System(s) or Authorized Devices, or which may constitute a Breach.

3.2.7.2. *Subscriber Investigation*. Each Subscriber shall investigate any reported Security Incident or Unauthorized Use or Disclosure involving access to or use of Services (i) from or by use of Subscriber's Information System or any other equipment or device of Subscriber, Authorized or otherwise, (ii) by use of a user name and/or password issued to a User of the Subscriber, or (iii) by a User of the Subscriber contrary to the Underlying Agreement, applicable Business Associate Agreement, this Policy or the Terms of Use, promptly upon receiving notice from CMT or other information which reasonably indicates the occurrence of such an event. The Subscriber shall document the results of each such investigation. The Subscriber shall permit CMT to review such documentation on a reasonable basis and shall promptly report to CMT any Security Incident or Unauthorized Use or Disclosure which presents or indicates a potentially material threat to Services or any other Subscriber's Protected Health Information, Information System(s) or Workstations or other equipment or devices, or which may constitute a Breach.

3.2.7.3. *Cooperation in Investigations*. CMT and all affected Subscribers shall share information about the results of their investigations under this Section and cooperate in determining and implementing measures to mitigate the harmful effects of any given event and prevent other events of the same type, to the extent practicable.

3.2.7.4. *Law Enforcement Notification*. Any party may notify appropriate law enforcement agencies in the event it believes a Security Incident or Unauthorized Use or Disclosure which affects it is a crime or the result of criminal activity.

3.3. Breach Notification.

3.3.1. *Breach Determination*. The Covered Entity whose Protected Health Information was affected by an Unauthorized Use or Disclosure, or the Covered Entity's designee if applicable, shall be responsible for making a determination whether the event constitutes a Breach under Federal or state law. Any other affected party may also make such a determination, at its discretion, and any affected party may make a determination whether or not the event constitutes a breach requiring notification under any state law.

3.3.2. If CMT determines that an Unauthorized Disclosure constitutes a breach under State law, CMT shall immediately notify the Subscriber of this determination.

3.3.3. *Terms of Notification*.

3.3.3.1. Each affected Subscriber which has a direct provider-patient, plan- member/participant or entity-customer relationship with potentially affected individuals shall have primary responsibility for their notification, if required by law or elected by the Subscriber.

3.3.3.2. Each affected Subscriber is primarily responsible for notification of regulatory authorities, if required by law or elected by the Subscriber.

3.3.3.3. Any notification to potentially affected individuals or to regulatory authorities shall be deemed notification as well by CMT (and any affected Subcontractor, if applicable) and each shall be identified as a notifying party, unless such party directs otherwise in writing.

3.3.3.4. In the event an affected Subscriber elects not to or fails to timely notify potentially affected individuals or regulatory authorities as provided above, and CMT reasonably determines that it may be required to give such notification by law, CMT may give such notification at its discretion.

3.4. CMT Remedies for Subscriber Security Failure. In the event that CMT determines that a failure by a Subscriber to comply with Section 2 of this Security Policy creates a material vulnerability potentially affecting (i) Services, (ii) the Information System or any other equipment or device of any party, or (iii) any information, including but not limited to Protected Health Information, CMT shall promptly notify the Subscriber and may, at CMT's reasonable discretion, suspend or limit access to and/or use of Services by some or all of the Subscriber's Users, and/or to or from the Subscriber's Information Systems and/or Authorized Devices), as CMT may determine is reasonably prudent. Such a failure by the Subscriber shall be deemed a Curable Breach under the Underlying Agreement, provided that upon receipt of notice of such a breach the Subscriber shall use its best efforts to come into compliance with this Policy. Upon the Subscriber's demonstration to CMT that the Subscriber is in compliance with this Policy CMT shall terminate the suspension or limitation unless other information available to CMT indicates that the material vulnerability continues. In the event of a continuing failure to come into compliance by the Subscriber, CMT may proceed to terminate the Agreement as provided therein.

3.5. Subscriber Remedies for Services Security Failure. In the event that the Subscriber determines that a failure by CMT to comply with Section 1 of this Policy creates a material vulnerability potentially affecting (i) the Subscriber's Information System or (ii) any information, including but not limited to Protected Health Information, accessible in or through the Subscriber's Information System, the Subscriber shall promptly notify CMT and may, at the Subscriber's sole discretion, suspend or limit access to and/or use of Services by some or all of the Subscriber's Users, and/or from the Subscriber's Information System(s), as the Subscriber may determine is reasonably prudent in order to mitigate the vulnerability. Such a failure by CMT shall be deemed a Curable Breach, provided that upon receipt of such notice CMT shall use its best efforts to come into compliance with this Policy. Upon CMT's demonstration to the Subscriber that CMT is in compliance with this Policy the Subscriber shall terminate the suspension unless other information available to the Subscriber indicates that the material vulnerability continues. The Subscriber shall not be liable for any fees payable for Services during any period of suspension under this Section, or for any reactivation fees following such suspension.