TCA Information Security Requirements For TCA partner(s)

DRAFT VERSION

May 20, 2018

INFORMATION SECURITY REQUIREMENTS

1. TCA Partner shall maintain the privacy of personal information and confidential data as confidential information. TCA Partner shall not use, disclose, or release confidential information contained in TCA records without permission from the TCA Board of Directors.

2. TCA Partner shall maintain the privacy of confidential information and shall be financially responsible for any notifications to affected persons (after prompt consultation with the TCA) whose personal information was disclosed by any security breach relating to confidential information resulting from TCA Partner's or its personnel's acts or omissions.

3. TCA Partner is required to maintain adequate security sufficient to protect sensitive TCA data to which they have access.

4. TCA Partner shall require all its affiliates and subcontractors, as a condition to their engagement, to protect all sensitive TCA data.

5. TCA Partner shall not use or disclose TCA Protected Data other than to carry out the purposes of this agreement.

6. TCA Partner shall not disclose any TCA Protected Data other than on a "need to know" basis.

7. TCA Partner shall develop, implement, maintain and use appropriate administrative, technical and physical security measures, which may include but not be limited to encryption techniques, to preserve the confidentiality, integrity and availability of all such TCA Protected Data.

8. Upon the termination or expiration of this Agreement, or at any time upon the request of the TCA, TCA Partner and its subcontractors shall return all TCA Protected Data (and all copies and derivative works thereof made by or for TCA Partner). Further, TCA Partner and its subcontractors shall delete or erase such TCA Protected Data, including copies and derivative works thereof, from their computer systems.

9. TCA Partner shall report, in writing, to the TCA any use or disclosure of TCA Protected Data not authorized by this Agreement or authorized in writing by the TCA, including any reasonable belief that an unauthorized individual has accessed TCA Protected Data. This report shall be made to the TCA's primary contact and TCA's Board of Director. It shall include details relating to any known or suspected security breach of TCA Partner's system or facilities which contain TCA Protected Data or any other breach of Protected Data relating to this Agreement. This report shall be made than within two (2) days after discovery, if the information was, or is reasonably believed to have been, acquired by an unauthorized person.