TRESORIT

BUSINESS ASSOCIATE AGREEMENT
WITH BUSINESS ASSOCIATE

This Agreement is made effective the ____ day of _________, 2016, by and between ___________________________, a ______________________ corporation duly authorized and existing in the State of ____, United States of America ("Client") and Tresorit AG, a corporation duly organized and existing in Switzerland, (hereinafter referred to as "Tresorit").

WITNESSETH:

WHEREAS, Client has entered into a service agreement with a business entity constituting a "Covered Entity" as defined under the federal Health Insurance Portability Act of 1996 (HIPAA) pursuant to which Client provides certain services to the Covered Entity and creates or receives certain confidential protected health information ("PHI"); and

WHEREAS, Client and Tresorit have entered into an agreement involving certain business cloud storage, sync and share services and related software ("the Services") through which Client shall encrypt the PHI of the Covered Entity's patients and/or customers, and then transmit the encrypted PHI to the Tresorit cloud service; and

WHEREAS, the parties acknowledge and agree that the Services do not extend to Tresorit Premium or Basic Services or other Tresorit non-business products which have limited control features compared to the Tresorit Business products; and

WHEREAS, the Services and relevant terms and conditions are further described and set forth in the Tresorit Standard Terms and Conditions of Use as posted on the Tresorit web page _ HYPERLINK "https://tresorit" _https://tresorit_, (version 10/7/2014) ("Terms and Conditions") as it may be amended from time to time, all of which are incorporated herein by reference and acknowledged by the parties to be binding and enforceable provisions; and

WHEREAS, Client acknowledges that Tresorit does not offer back-up services; but rather a cloud storage sync and share service and that (i) Client is responsible for back up of all Covered Entity and/or Client data; (ii) Tresorit's client-side encryption makes the files provided by Client secure before they leave the Client location and does not permit decryption in the cloud; and (iii) the only persons with the decryption key and with access to the PHI are those persons specifically designated and provided access by Client and/or Covered Entity; and

WHEREAS, the parties recognize and agree that the American Recovery and Reinvestment Act of 2009 (ARRA), including the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. 17921-17954 (HITECH), and the Health Insurance Portability Act of 1996 (HIPAA), both of which address the protection of PHI and impose standards for the privacy of individually identifiable health information, 45 C.F.R. 164.504 ("the Privacy Rule") and the security of electronic protected health information ("the Security Rule"), including with respect to : (a) Administrative Safeguards (45 CFR § 164.308); (b) Physical

Safeguards (45 CFR § 164.310); (c) Technical Safeguards (45 CFR § 164.312); (d) Policies and Documentation (45 CFR § 164.316); and (e) Breach Notification requirements (HITECH ACT, § 13402) all jointly referred to herein as the "HIPAA and HITECH Laws and Regulations" require Covered Entities and their Business Associates, as defined in the HIPAA Laws and Regulations, to protect PHI from unauthorized disclosure; and

WHEREAS, the HIPAA and HITECH Laws and Regulations define a Business Associate as a person who creates, receives, maintains, or transmits PHI for a function or activity on behalf of a Covered Entity (or on behalf of a Business Associate of a Covered Entity), including data transmission services; and

WHEREAS, Client is obligated to provide assurance to Covered Entity that Client's contractors who may be Downstream Business Associates of Client by virtue of having access to the PHI of the Covered Entity, shall abide by the HIPAA and HITECH Laws and Regulations; and

WHEREAS, although Tresorit stores PHI in an encrypted form using zero-knowledge technology in its Business products, and thus does not have access to identifiable data, Client and Tresorit agree to enter into a Business Associate Agreement only to the extent that Tresorit is considered a Downstream Business Associate and ever accesses or uses unencrypted PHI of Covered Entity or of Client; and

THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree to the provisions of this Business Associate Agreement.

I. **DEFINITIONS**.

Except as otherwise defined herein, any and all capitalized terms in this Section shall have the definitions set forth in the HIPAA Security and Privacy Rule. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Security and Privacy Rule, as amended, the HIPAA Security and Privacy Rule shall control. Where provisions of this Agreement are different than those mandated in the HIPAA Security and Privacy Rule, but are nonetheless permitted by the HIPAA Security and Privacy Rule, the provisions of this Agreement shall control.

The term "Protected Health Information" or "PHI" means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. "Protected Health Information" includes without limitation "Electronic Protected Health Information".

"Electronic Protected Health Information" or "EPHI" means Protected Health Information which is transmitted, stored or maintained by Electronic Media (as defined in the HIPAA Security and Privacy Rule).

II. CONFIDENTIALITY AND SECURITY REQUIREMENTS.

2.01 **Scope of Agreement**. Tresorit acknowledges and agrees that all PHI that is created or received by Client and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display by Client to Tresorit or is created or received by Tresorit on Client's behalf shall be subject to this Agreement. Tresorit acknowledges that Client is relying on the administrative, physical and security safeguards of Tresorit in selecting Tresorit to provide Services. Tresorit further acknowledges that sections of HIPAA and the HITECH Act, including the Privacy Rule and the Security Rule, may apply directly to Tresorit, just as the provisions apply to Client, to the extent Tresorit transmits or maintains PHI, and Tresorit agrees to comply with such rules and regulations. Tresorit may use or disclose PHI as necessary to perform its obligations under this Agreement and the Terms and Conditions but only to the extent that such uses are permissible under HIPAA, including but not limited to the Privacy Rule.

2.02 **Obligations Imposed by Agreement**. Without limiting any other requirements set forth in this Agreement, to the extent Tresorit receives, maintains, or transmits unencrypted PHI and such PHI is in its possession and control, Tresorit shall:

(a) protect and safeguard from any verbal and written disclosure all confidential information regardless of the type of media on which it is stored (e.g., paper, fiche, electronic) with which it may come into contact; implement and maintain appropriate policies and procedures to protect and safeguard the PHI;

(b) implement appropriate safeguards to prevent use or disclosure of Protected Health Information other than as permitted in this Agreement;

(c) implement administrative, physical, and technical safeguards that are compliant with the HIPAA and HITCH Security Laws and Regulations to protect the confidentiality, integrity, and availability of any EPHI that it creates, receives, maintains, or transmits on behalf of Covered Entity;

(d) use or disclose any PHI solely: (1) for meeting its obligations as set forth in any agreements between the parties evidencing their business relationship, or (2) as required by applicable law, rule or regulation, or by accrediting or credentialing organizations to whom Client or Covered Entity is required to disclose such information, and (3) as would be permitted by the HIPAA Security and Privacy Rule if such use or disclosure were made by Client or Covered Entity;

(e) ensure that its agents, including subcontractors to whom it provides PHI, agree to the same restrictions and conditions that apply to Tresorit with respect to such information, and agree to implement reasonable and appropriate safeguards to protect any such information; and

(f) take reasonable steps to ensure that Tresorit's employees' actions or omissions do not cause Tresorit to breach the terms of this Agreement.

(g) provide access to Client, and in the time and manner reasonably designated by Client, to any unencrypted PHI in a Designated Record Set, if any is held by Tresorit, in order to meet the requirements or to assist Covered Entity or Client in meeting the requirements, under 45 CFR §164.524.

(h) utilize where available, health information technology systems and products that meets standards and implementation specifications adopted under §3004 of the Public Health Service Act, as added by §13101, whenever Tresorit implements, acquires or upgrades its health information technology systems.

(i) make internal practices, books, and records relating to the use and disclosure of PHI received from Client available to either the Client for review purposes, or to the Secretary, for purposes of the Secretary determining Covered Entity's or Client's compliance with the Privacy Rule.

(j) disclose to its subcontractors, agents or other third parties only the minimum PHI (if any) necessary to perform or fulfill a specific function required or permitted hereunder.

2.03 **Allowable Uses of PHI.** Notwithstanding the prohibitions set forth in this Agreement, Tresorit may use and disclose PHI, if any is stored or maintained by Tresorit, as follows:

(a) for the proper management and administration of Tresorit or to carry out the legal responsibilities of Tresorit, provided that as to any such disclosure, the following requirements are met:

(1) the disclosure is required by law: or

(2) Tresorit obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Tresorit of any instances of which it is aware in which the confidentiality of the information has been breached.

(b) for data aggregation services, if to be provided by Tresorit for the health care operations of Covered Entity pursuant to any agreements between the Parties evidencing their business relationship. For purposes of this Agreement, data aggregation services means the combining of PHI by Tresorit with the protected health information received by Tresorit in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

III. AVAILABILITY OF PHI FOR COVERED ENTITY.

The parties recognize and agree that Client and not Tresorit has access to unencrypted PHI. However, in the event and to the extent that Tresorit ever has access to unencrypted PHI, Tresorit agrees to make the PHI available to Covered Entity and/or Client (i) to the extent and in the manner required by the HIPAA Privacy Rules (i) §164.524 regarding patient access to records; (ii) §164.526 for amendments to PHI; and (iii) §164.528 regarding accounting of disclosures. Accordingly, the Secretary of Health and Human Services shall have the right to audit Tresorit's records and practices related to the use and disclosure of PHI to support Covered Entity's compliance with the terms of the HIPAA Security and Privacy Rule. The parties agree that the availability of encrypted PHI is subject to the Terms and Conditions.

IV. TERM AND TERMINATION

4.01 **Term**. The Term of this Agreement shall be effective as of the Effective Date and shall continue in effect until all of the PHI provided by Client to Tresorit, or created or received by Tresorit on behalf of Client, is destroyed or returned to Client, and all obligations of the parties have been met, unless terminated by mutual written agreement of the parties or as otherwise provided herein.

4.02 **Termination Rights**. Notwithstanding anything in this Agreement to the contrary, Client shall have the right to terminate this Agreement and the parties business arrangement (and any related contract) immediately (a) if Client determines that Tresorit has violated any material term of this Agreement; or (b) if Tresorit fails to provide adequate written assurances to Client that it will not breach this Agreement, within a reasonable period of time following receipt of notice from Client of Client's belief that a breach, whether inadvertent or intentional, is threatened by the acts or omissions of Tresorit.

4.03 **Effect of Termination.** Tresorit shall return all PHI to Client within 30 days of the termination of this Agreement, including PHI that is in the possession of subcontractors or agents of Tresorit. In the alternative, Client may agree to certification of the destruction of the PHI. In any event, Tresorit shall retain no copies of the PHI. In the event that Tresorit determines that returning or destroying the PHI is infeasible, Tresorit shall provide to Client notification of the conditions that make return or destruction infeasible. In that event, Tresorit shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Tresorit maintains such PHI.

V. REPORTING OF DISCLOSURES.

Tresorit shall timely report to Client any Security Incident involving unencrypted PHI within its possession or control, in accordance with the HITECH Act, 42 U.S.C. 17932(b). Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations which threatens to or does cause the disclosure of unencrypted PHI.

5.01 **Recordkeeping.** Tresorit agrees to document disclosures of PHI as would be required for Client as a Business Associate under HIPAA or HITECH, to facilitate an accounting of disclosures of PHI by Client or Covered Entity, including in accordance with 45 CFR §164.528 and the HITECH Act §13405 codified at 42 USC §17935.

5.02 **Timing of Notifications to Client**. Notwithstanding any less restrictive requirements herein or in applicable regulations, Tresorit agrees to make information regarding disclosures, if any, of unencrypted PHI available to Client within:

(a) fifteen (15) days of a request by Client. Tresorit shall provide, at a minimum, the following information, if known to Tresorit: (i) the date of disclosure; (ii) the name of the entity or person who received the PHI, and the address of such entity or person if known; (iii) a brief description of the PHI disclosed; (iv) a brief statement regarding the purpose and explanation of the basis of such disclosure; and (v) the names of all individuals whose PHI was disclosed.

(b) fifteen (15) business days of a request by the Client, Tresorit agrees to comply with Client's request to accommodate an individual's access to his/her PHI. In the event an individual contacts Tresorit directly about access to PHI, Tresorit shall forward such request to Client within three (3) business days and shall respond pursuant to instructions from Covered Entity.

5.03 **Notifications to public and/or patients**.

(a) Client, as the sole party with access to unencrypted identifying information, agrees to be responsible for carrying out any notifications required to be made pursuant to applicable laws and regulations in the event of an unauthorized disclosure of PHI.

(b) Tresorit agrees to bear the costs of any notifications required to be made pursuant to applicable laws and regulations in the event of an unauthorized disclosure of PHI caused solely by the negligent or other wrongful act or omission by Tresorit or its employees or agents.

(c) The costs of any notifications other than those referenced under 5.03(b) shall be the sole responsibility of Client.

VI. <u>INDEMNIFICATION.</u>

6.01 **Client Obligations**. Client agrees to indemnify and hold Tresorit harmless from any and all claims or losses arising from Client's business operations including but not limited to any claims involving an alleged unauthorized disclosure of PHI, or the violation of any obligation under HIPAA or the HITECH Act.

6.02 **Tresorit Obligations**. Tresorit agrees to indemnify and hold Company harmless from any and all claims or losses arising from an alleged unauthorized disclosure of unencrypted PHI, or the violation of any obligation under HIPAA or the HITECH Act if and to the extent caused solely by wrongful acts or omissions of Tresorit in maintaining, storing or transmitting PHI.

6.03 **Attorney Fees**. Indemnification obligations under this Agreement shall include reimbursement for attorney fees incurred by the indemnified party in responding to any claims asserting a breach of any HIPAA or HITECH provisions, or in enforcing any provision of this Agreement. This provision shall survive the termination of this Agreement

VII. MISCELLANEOUS

7.01 **No Rights in Third Parties.** Except as expressly stated herein or the HIPAA Security and Privacy Rule, the parties to this Agreement do not intend to create any rights in any third parties.

7.02 **Amendments**. This Agreement may be amended or modified only in a writing signed by the parties.

7.03 **Assignments**. No party may assign its respective rights and obligations under this Agreement without the prior written consent of the other party.

7.04 **Governing Laws**. This Agreement will be governed by the federal laws of the United States and the State of Maine to the extent any State law applies. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasion shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

7.05 **Enforceability**. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

CLIENT:

____
By:_____________________________
Title: ___________________________

TRESORIT:

____
By:_____________________________
Title: ___________________________