WinterLight Privacy Notice

Effective: 1 January, 2018

At WinterLight, we take the privacy and security of your information seriously. We aim to be clear and open about our policies. If you have any questions regarding our privacy and security practices, please contact our Chief Privacy and Security Officer at privacy@winterlightlabs.com.

February, 2018. Update re: Spectre/Meltdown.

To address the recently discovered vulnerabilities affecting most modern processors (Spectre and Meltdown), we have patched all of our servers and company devices to the latest OS / kernel version which provides mitigation against all three variants of the threat.

Personal information and personal health information

Personal information (PI) refers to information which can be used to identify you, such as your name, email address, or a recording of your voice.

Personal health information (PHI) is a subset of PI, which identifies your health history and use of health services. This is also known as *protected health information* in the United States. In the European Union, *personal data* refers to both PI and PHI.

Collection

WinterLight may collect one or more of the following types of PHI:

- Audio recordings of your voice
- Typed responses to linguistic tasks
- Demographic data (e.g., your month and year of birth and your sex)
- Your health history (e.g., cognitive and neuropsychiatric assessments, and diagnoses if applicable)

Use

WinterLight may collect and use PHI for one or more of the following purposes:

- Assist your healthcare provider(s) and caregiver(s)
- Improve WinterLight's internal data processing, speech recognition, and machine learning algorithms, and statistical models used for analysing PHI, in order to allow us to continuously improve the services we offer
- Conduct academic research in compliance with protocols approved by a Research Ethics Board (REB) or an Institutional Review Board (IRB)

Privacy

Privacy, the right of individuals to be free from unwarranted intrusions into their personal lives, is important to us. We have policies in place to ensure the privacy of your information, which includes the protection of PI and PHI, as well as how it is transmitted, stored, used, and disclosed. We adopt the *CSA Model Code for the Protection of Personal Information* as a guiding principle when developing our information privacy policy.

We only give access to your information to company staff who require it as part of their job responsibilities. Staff are only allowed to access your information for an authorized purpose. Employees who are responsible for maintaining our infrastructure have access to the systems which store and process client information, such as our databases, in order to allow them to perform tasks like database upgrades and maintenance. These employees are prohibited from using these permissions to view the data unless it is necessary to do so as part of their job (e.g., to verify data integrity after an upgrade). We have access logging and other technical controls in place to allow us to monitor for unauthorized access or unacceptable use of the data.

We store your data on infrastructure provided by our cloud service provider, Amazon Web Services (AWS), and we have an executed business associate agreement (BAA) with them – this agreement requires AWS to appropriately safeguard the data with the same or comparable level of protection as we do.

If we collect any paper-based data, such as cognitive assessments, we store the papers in locked cabinets. We require our employees to maintain a "clean desk" policy, which means storing all confidential materials in locked cabinets, as well as locking their workstations, laptops and other devices each time they leave their work area.

We do not disclose your information to any third parties, unless you expressly consented to it (e.g., if you are participating in a research study at a retirement home you may consent to disclosing information to a staff physician if we uncover information that suggests you may have an undiagnosed condition) or as required by law (e.g., if the data was collected as part of a research study, it may be reviewed for quality assurance by representatives of the Human Research Ethics Program to make sure that the required laws and guidelines are followed).

Security

We adopt the *ISO/IEC 27002:2013 (Code of Practice for Information Security Controls)* as our guide to developing and deploying our information security management program.

Infrastructure

We use only HIPAA-eligible AWS services, and we have an executed BAA with AWS. We use a variety of technical controls following best practices for network security, such as blocking of unnecessary ports on our servers through AWS security groups and performing regular scans of

our servers to detect network vulnerabilities (e.g., insecure data transmission protocols and expired digital certificates).

Data

We use the latest recommended secure cipher suites and protocols for data encryption in transit. Data is encrypted at rest.

Where applicable, based on regulatory and client requirements, we store collected data in the appropriate country or region.

Models

Unless indicated otherwise in a client agreement or data consenting process, aggregated and non-personally identifying data derivatives, such as variables we calculate from the raw data samples (e.g., number of nouns or duration of pauses), may be used to train cross-dataset statistical models. Such statistical models are trained and stored in the US data region on our cloud infrastructure, and may be used to provide services in any region.

Logging

We maintain extensive logs with respect to every component of our services, including applications, application programming interfaces (APIs), cloud services, servers, and management consoles. The logs contain information pertaining to security, monitoring, access, and other operational metrics. The logs are reviewed for privacy and security events on a periodic basis.

Authentication

Our mobile applications are protected with user credentials. User passwords must meet our password policy, which has requirements for password strength, length, and regular password rotation. Our APIs implement the standard OAuth2 authentication protocol.

Devices

Company devices (e.g., workstations and laptops used by employees and contractors) have enabled firewall, up-to-date antivirus software with regularly scheduled scans, automatic OS security updates, disk encryption, and auto-locking after a period of inactivity.

Personnel practices

All of our employees and contractors who have access to your information meet the following requirements:

- Complete a background check
- Sign a confidentiality agreement
- Receive privacy and security training

Disaster recovery

We use production databases with replication across multiple availability zones to ensure redundancy and smooth failover in the case of infrastructure failure in one zone. We use versioning and replication across multiple regions for our file storage solution to ensure high availability. This means that in the event of an infrastructure failure in one zone or region, our services should continue working with minimal downtime.

Incident Management and Response

We have an incident management policy and procedures in place to prevent, detect, respond to, and contain privacy/security incidents or breaches. In the event of a detected and confirmed privacy or security breach (e.g., your information was subject to unauthorized use or disclosure), we will promptly notify either your healthcare provider (if they provided your information to WinterLight, in which case it is their responsibility to notify you) or yourself (if you provided your information to WinterLight directly).

As part of our policy for prevention of privacy/security breaches, we contract an independent external privacy and security firm; we are currently undergoing a privacy impact assessment (PIA) of our services.

Access

You have the right to request access to the PHI which we store about you. Additionally, you can request corrections and updates to be made to it – for example, if your birth date was entered incorrectly you can provide a correction. To request access or corrections to your information, follow the case that applies to you:

- Case 1: If your information was supplied to WinterLight by your healthcare provider or organization, then you should contact them directly.
- Case 2: If you provided your information to WinterLight yourself, then you can send a request for access or corrections to our Chief Privacy and Security Officer at privacy@winterlightlabs.com.