<center>**Security Measures**</center>

BrightInsight maintains an information security program (including the adoption and enforcement of internal policies and procedures) designed to identify reasonably foreseeable and internal security risks and unauthorized access to the BrightInsight Platform (the "Platform"), and to remediate or mitigate security risks in priority of likelihood and severity.

The BrightInsight Platform is routinely assessed by a Third-Party Auditor in accordance with HITRUST, ISO/27001, and HDS (Hébergeur de Données de Santé) certification requirements.

Access Controls

(a) Data Center Access Controls.

Cloud Data Centers. Google Cloud Platform ("GCP") is used to provide infrastructure services to host and operate the Platform. By using GCP, BrightInsight is able to take advantage of GCP's sophisticated security environment.

Physical Access Control. Cloud data centers used for the Platform maintain on-site security operations responsible for all physical data center security functions 24 hours a day, 7 days a week, with CCTV monitoring and access controls. These data centers are Tier 3 certified, SOC 2 Type II computing facilities.

(b) Logical and Data Access Controls.

Security Personnel. BrightInsight's dedicated team of security personnel is responsible for the ongoing monitoring of BrightInsight's information security program, personnel, infrastructure, and Platform, and for responding to security incidents, identified risks and regulatory changes.

Internal Data Access Processes and Policies. BrightInsight's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process data on the Platform.

Access Management. BrightInsight employs a centralized access management system to control personnel access to production servers for the Platform to a limited number of authorized personnel. Central network-based authentication systems are designed to provide BrightInsight with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information for the Platform. BrightInsight requires the use of unique user IDs, strong passwords, two factor authentication, and access lists for BrightInsight personnel to access the Platform. The granting or modification of access rights to the Platform by BrightInsight personnel is based on: (i) the authorized personnel's job responsibilities; (ii) job duty requirements necessary to perform authorized tasks based on least privilege; and (iii) a need to know basis. The granting or modification of access rights must also be in accordance with BrightInsight's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Logins to the Platform are logged into SIEM.

Access Controls. Security events for the Platform, including login failures, changes to access models or file permissions, modification to installed software or operating systems, changes to user permissions or privileges are logged on the relevant systems. Logs are generated through monitoring and alerting systems.

Network Security

(a) Data Transmission. BrightInsight makes HTTPS encryption (also referred to as TLS connection) available for data in transit to or from the Platform. Clear text HTTP connections to the Platform is disabled by default.

(b) Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. BrightInsight intrusion detection involves: controlling the size and make-up of BrightInsight's attack surface through preventative measures; employing intelligent detection controls at data entry points; and employing technologies that automatically remedy certain dangerous situations.

Application Security

(a) Software Development. BrightInsight employs a static code review process to increase the security of the code used to provide the Platform. All development for the Platform is based on Software Development Lifecycle (SDLC) procedure (part of the Brightinsight Quality Management System).

(b) <u>Standards Compliance</u>. BrightInsight follows OWASP Top 10 best practices and NIST800, ISO27001, and HITRUST standards.

(c) <u>Data Integrity</u>. Measures are in place to prevent corruption of stored Customer Data due to a malfunctioning of the Platform. These include, patch management and change control procedures, QA testing prior to release, and logging of all changes to production systems for the Platform.

Customer Data

(a) <u>Data Storage and Isolation</u>. BrightInsight stores Customer Data in completely separate cloud environments (single-tenant) on public cloud infrastructure to ensure the isolation of Customer Data. Even within the single-tenant instance for a customer's product, the BrightInsight Platform separates identifiable and non-identifiable data in different cloud environments.

(d) <u>Pseudonymization and Encryption</u>. The Platform includes configurations in order to reduce direct references to persons during processing in such a way that it is only possible to associate data with a specific person if additional information is included. The additional information is kept separately from the pseudonym by appropriate technical and organizational measures in place. The Platform uses databases that are encrypted per industry standard.

Data Breach Management

If BrightInsight becomes aware of a Data Breach, BrightInsight will notify Customer without undue delay of the Data Breach and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Breach will be delivered to the email address provided by Customer in the Agreement. "Data Breach" means a breach of security of the Platform leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on the Platform, and does not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems; or (ii) breach of security not caused by BrightInsight.

Personnel Security

(a) <u>Background Checks</u>. BrightInsight conducts appropriate background checks of our employees to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

(b) <u>Employee Training</u>. BrightInsight employees are required to execute acknowledgment of its Acceptable Use Policy and undergo new hire and annual security training.

(c) <u>Employee Code of Conduct</u>. BrightInsight employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

Privacy by Design

BrightInsight employs Privacy by Design and Privacy by Default principles in its development and operations processes.

Authorized Subprocessors

(a) Subprocessor Security. Prior to onboarding subprocessors, BrightInsight conducts a commercially reasonable selection process by which it evaluates the security, privacy and confidentiality practices of subprocessors to assess that subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.