TERMS AND CONDITIONS

The following are Terms for Primordial products and services. If you have any questions, please contact Support or your Account Manager.

Customer agreements and user terms for products and services

Data Processing Agreement

DATA PROCESSING DETAILS

(a) The subject matter, nature and purpose of the Processing is delivery of the Services to Company in accordance with Primordial's published product documentation for the product in question. Company gives Primordial the right to anonymize the personal data in accordance with applicable law and/or to de-identify the personal data in accordance with 45 C.F.R. §164.514 or other applicable law. Company instructs Primordial and its service providers/sub-processors and Affiliates to use, compile (including creating statistical and other models), annotate and otherwise analyze the personal data to develop, train, tune, enhance and improve the natural language processing and other components of Primordial's software and technologies embodied in the Services.

(b) The categories of Data Subjects may include (1) patients or clients who receive medical

care from the Company, (2) Company personnel, including doctors, nurses, administrators, medical personnel and other authorized individuals who use the Services, and (3) employees, agents.

(c) The types of Personal Data Processed are under the control of Company as Controller and will depend on the categories of Personal Data Processed by Company using the Services, but will likely include name, date of birth, medical record number, other identification numbers, age, and the basic elements of the radiology report. Additionally, Personal Data of Company personnel will also be Processed, including name, contact information and voice recordings.

(d) The categories and types of Personal Data involved and transferred may include sensitive personal data, which may include but is not limited to health data. Primordial's technical and organization measures are designed from ground-up to ensure appropriate handling and protection of sensitive personal data.

(e) Data Centers for Processing of Personal Data will be in the following locations: United States

(f) The retention period is the duration of

(i) the Main Agreement in case of a DPA for End Users;

(ii) the Terms of Service in case of a DPA for Primordial Services; and

Any data retention period specified in the above terms, as applicable, or by law (or, if no specific data retention period is specified in the above terms, the data retention period specified by Primordial data retention and destruction policy.

(g) The frequency of the transfer depends on the frequency the Service is used by Company and will likely be recurrent.

Sub-Processor List

Primordial engages the following entities to assist in connection with the Services as specified below:

Primordial Affiliate Sub-Processors

Entity Name	Contact Details	Processing Activities and Location(s)
Microsoft Corporation and affiliates	One Microsoft Way Redmond, Washington 98052 United States www.microsoft.com	The MS Azure Cloud Services Platform is used for the hosting of data and the mPower application is used for natural language understanding of unstructured data. Locations: United States.

TECHNICAL AND ORGANIZATIONAL MEASURES

Primordial maintains appropriate technical and organizational measures, through the implementation and enforcement of the following policies:

Security Organization, Risk Analysis and Risk Management
Primordial has a professional information security organization, headed by a Chief Information Security Officer, that works to provide robust information security controls for Primordial products and environments. Primordial performs annual assessments of the compliance of Primordial security controls with current certifications and industry standard controls.

Workforce Clearing, Training and Sanctions
All Primordial personnel are subject to background checks before access to restricted data is permitted. All personnel receive regular security training. Primordial has adopted policies and procedures to apply workforce sanctions to employees who fail to comply with Primordial security policies and procedures.

Physical Controls
Primordial Data Centers - All Primordial facilities are protected by physical security controls including perimeter controls, electronic access systems, locks and cameras. Primordial stores all production data in physically secure data centers that also maintain additional access restrictions, including: caged, locking racks along with secondary authentication and access. Primordial's infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks.

Cloud Data Center - Microsoft Azure runs in data centers managed and operated by Microsoft. These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The data centers are managed, monitored, and administered by Microsoft operations staff. The operations staff has years of experience in delivering the world's largest online services with 24 x 7 continuity. For additional information, please refer to https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.

Access
Primordial has located all equipment that stores Personal Data in controlled access areas. Primordial will only allow employees and contingent workers with a business purpose to have access to such controlled areas.

Access Points
Primordial's externally-facing web servers and third-party access points are configured securely, including (but not limited to) implementing a properly constructed dedicated firewall, requiring a virus check before granting access to any third-party network, and disabling or removing routing processes to minimize access.

Business Continuity, Disaster Recovery
Primordial has implemented and documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services in a timely manner after a disruptive event. Primordial regularly tests and monitors the effectiveness of its business continuity and disaster recovery plans.

Network Security
Primordial has implemented appropriate supplementary measures to protect Personal Data against the specific risks presented by the Services. All data is protected by encryption in transit over open, public networks. Data at rest is protected either by encryption or compensating security controls, which include pseudonymization, segmented networks, tiered architecture, firewalls with intrusion protection and anti-malware protections, and

limiting of port access. Personal Data is only retained for the duration required for regulatory purposes, unless otherwise outlined by the Services.

Portable Devices
Primordial will not store Personal Data on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks, USB or flash drives, personal digital assistants (PDAs) or mobile phones, DVDs, CDs or computer tapes) unless it is encrypted with a minimum of 128-bit, or such higher bit encryption in accordance with then current industry best practice. Primordial endpoints are provisioned with a default configuration, enforced at the organizational level.

Monitoring
Primordial takes appropriate steps to monitor the security of Personal Data and (if appropriate) to identify patterns of suspect activity. Primordial designs applications and services to suppress sensitive data being stored by Primordial. For every identified hosted change, security and QA teams review the data mapping requirements to validate the intended fields continue to be suppressed. Primordial also monitors security logging events which include log-on violations or attempts. Data retained from logs includes, but is not limited to, timestamp, hostname, and username for accountability.

Data Subject Requests
Primordial implements a documented process for assisting Company in responding to Data Subject Requests.

Governmental Requests
Primordial will not disclose or provide access to Personal Data being Processed under this DPA to law enforcement, unless required to by law, and only upon service of a legally-binding request or order from a governmental authority.

If compelled to disclose or provide access to any Company Data to law enforcement, Primordial will promptly notify Company and provide a copy of the demand unless legally prohibited from doing so.

Physical Controls
Risk inherent to organizational premises. Facilities hosting information systems must have appropriate security controls including but not limited to access controls, security officers and cameras. Managed facilities must implement adequate environmental safeguards to ensure availability and protect against damage. The physical and environmental safeguards will be evaluated, implemented and maintained regularly.

Access
Ability to control access to assets based on business and security requirements. A unique user identifier shall be created for each worker upon validation of the completion of the employment screening process. Password controls should follow industry standards. Privileged access must be allocated on a “need to know” basis and the access is commensurate to the user’s position and duties. Access to networks and network services, and sensitive information must use multi-factor authentication. Access must be logged and monitored for unauthorized usage or malicious intent. Access must be reviewed for access appropriate to role and terminations.

Network Security
Manage direction and support for information security in accordance with business requirements and relevant laws and regulations. Policies for information security approved, published and communicated. Policy review process with adoption and support of management.

Ability to ensure correct and secure operations of an organization’s assets.

- Hardware, operating system, database and applications must be actively supported by the vendor and receive regular security updates and maintenance.
- Information systems must have protection from malicious code with anti-virus and anti-malware with automatic updates.
- Industry-standard processes for Release, Change, Incident, and Problem management should be documented and implemented.
- Information assets should have auditing enabled and retained for a minimum of 1 year. Auditing logs should be protected from unauthorized access and monitored on a regular basis.

Compliance

Organization's ability to remain in compliance with regulatory, statutory, contractual, and security requirements.

- Maintain policies and procedures to ensure compliance of systems with regulations and standards.
- Compliance to any regulatory or security standards requirements where applicable (SOX, PCI-DSS, GDPR, etc.).
- Conduct periodic reviews and audits of information processing systems for compliance with information security policies and standards.

Asset Management

The ability of the security infrastructure to protect organizational assets.

- An inventory of assets with information and processing facilities shall be identified and maintained. Ownership should be identified with rules of acceptable use.
- Information classified with policies and controls applied appropriately to risk.
- The disposal of data should be done in a secure, protected way to ensure the inability to recover that data.

Information Systems Development and Maintenance

Ability to control access to assets based on business and security requirements.

- Project documentation for new information systems, or significant enhancements shall include security requirements and control as part of the functional requirements.
- Developer will include secure code testing as part of the Software Development Life Cycle (SDLC) with review of code.
- Input data processed shall be validated for correctness and security of data.
- Ensure the authenticity of the messages or transactional data through digital signatures and protect the integrity of the data through the use of industry standard encryption.

Information Security Incident Management
The organization should have the ability to recover from an information security incident.

- Employees will report incidents and follow an incident management process.
- The incident management process shall include identification, classification, impact analysis and an escalation process.
- The ability to perform post-mortem including follow-up drive to root cause with corrective action must be implemented.

PRIMORDIAL ACTIONABLE FINDINGS SMS TERMS & CONDITIONS

Primordial Actionable Findings is the **program name** for Primordial's SMS program. As a registered user, you can choose to opt-in to Primordial Actionable Findings SMS program. A **program description** is that the program allows registered users to receive urgent messages when they are away from their clinical workstation and need to be reached immediately.

The **frequency of messaging** will vary depending on your preferences. If you choose SMS as your primary message delivery option for Actionable Findings, then you will receive an SMS each time there is a critical finding sent to you from another physician. If you choose SMS as a secondary or backup means of communication, then you will only be contacted when you are unreachable on other means of communication, and the matter is urgent. If you have any questions about your text plan or data plan, it is best to contact your wireless provider.

Carriers are not liable for delayed or undelivered messages. Message and data rates may apply for any messages sent to you from us and to us from you.

You can cancel or **opt-out** of the SMS notifications at any time. Just text "STOP" in reply to the number (short-code) that sent you a message. After sending this, you will no longer receive SMS messages from Primordial. To rejoin, access your system administrator to resend a link via email or opt-in through your user preferences within the Communicator application.

If you are experiencing issues, you can reach out directly at 1-800-833-7776 or PDISupport@primordialdesigninc.com.

If you have any questions above privacy, please read our privacy policy here: Primordial Privacy Policy.