POLICY

Data Privacy

Compliance

Data Privacy

Policy Code	POL_PRV_1100
Version	V3
Effective Date	28/2/24
Approver	Eric Green

Purpose

This policy is designed to provide a global baseline across the Company with regards to the protection of Personal Information. It sets out the Company's commitment to ensuring that the processing of all Personal Information is carried out with integrity and in accordance with all relevant data protection law. Whilst it seeks to define our core purpose and principles without reference to any specific personal information protection regime, the Company recognizes that in certain jurisdictions the applicable regulations may impose additional, specific requirements: Where this is so, we will manage the processing and storage of Personal Information in accordance with all such applicable laws.

Scope

This corporate policy applies globally, to all employees, consultants, contractors, and vendors of Amplity Health, or of any of its current or future subsidiaries, affiliates, successors or assigns (collectively, the "Company"). All company workers are expected to comply with the policy. Failure to do so may lead to disciplinary action for misconduct, including dismissal or termination of contract.

The Policy covers:

- The processing and storage of Personal Information in electronic or paper format, including that belonging to employees, contractors, suppliers, clients, healthcare professionals, clinical investigators, patients, medical research subjects, consumers and other individuals where the Company is the Controller of their Personal Information.
- The processing and storage of Personal Information on behalf of our clients where the Company is a Processor of that information.

The Policy also applies to management and use of Personal Information in the form of electronic information (cookies, etc.) collected automatically during use of Company Websites. Further details are covered in a supplemental 'Online Privacy Policy' document.

Responsibilities

The Company has defined this and other related policies to ensure the delivery of good privacy and data protection practices. These include:

- Data Privacy Policy (this document)
- Online Privacy Policy
- Document Retention & Destruction Policy
- Access Control Policy
- Data Back-up Policy
- Data Classification Policy
- Information Security Policy

Policies are supported by Standard Operating Procedures (SOP) and Guidelines

Core Principles

The Company is committed to the principle of 'Privacy by Design' and seeks to ensure that good data protection practice is embedded in our culture and processes.

The Company complies with the fundamental principles of Personal Information protection set out below:

1. **Lawfulness, Fairness and Transparency (Notice)**
   We are clear, open, and honest about our use of Personal Information:
   - It is processed lawfully and in a manner that is not detrimental, unexpected, or misleading to the Data Subject.
   - Through appropriate Data Privacy Notices, we ensure that Data Subjects are aware of why and how their Personal Information is processed and used, of the lawful basis for processing and their rights under applicable data protection law.

2. **Choice**
   - We provide clear, conspicuous, and readily available mechanisms to enable Data Subjects to exercise their statutory rights to choose how their Personal Information is used. This includes the ability to opt out of (i) disclosure to a third-party Controller, (ii) use for a purpose materially different to the authorized purpose(s).
   - We facilitate, in good faith, any legitimate request from a Data Subject who wishes to exercise their rights under applicable data protection legislation.

3. **Limitation of Purpose**
   Personal Information is only collected and Processed when necessary, and for specified, explicit, and lawful purposes. It is not processed in a manner that is incompatible with those purposes, unless subsequently authorized by the Data Subject.

4. **Data Minimization**
   Only Personal Information that is adequate, relevant, and limited to what is necessary in relation to the stated purpose is collected.

5. **Accuracy**
   Personal Information that we hold is accurate and, where necessary, kept up to date. Reasonable steps are taken to ensure that inaccurate Personal Information is recognized and erased or rectified without delay, having regard to the purposes for which it is processed.

6. **Storage Limitation**
   Personal Information is kept in a form which permits identification of Data Subjects for no longer than is necessary to fulfill the legitimate purpose, or to comply with legal obligations.

7. **Integrity and Confidentiality**
   Personal Information is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures.

8. **Accountability**
   The Company takes full responsibility for complying with all relevant legislation by adopting this Policy and the other supporting Policies mentioned. Appropriate technical, organizational, and administrative measures are implemented and maintained, and records are kept to monitor and demonstrate compliance. Where relevant, the Company utilizes voluntary codes of conduct and certification schemes to maintain and improve the quality of delivery.

Our Use of Personal Information

The following table summarizes the various types of Personal Information that the Company may Process and share in the course of its normal business activities.

Category of Personal Information	Purposes	May be shared with
IDENTIFIERS: such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, government issued identifiers (e.g. social security number, device identifiers)	Operational purposes including internal management processes; business processes; recruitment; b2b marketing; service delivery; advertising	Affiliates and subsidiaries. Third-party service providers (processors) Clients, partners, sponsors and other third-party controllers (with consent) Ad networks and other third parties in the online advertising ecosystem (with consent) Legal authorities (when required by law)
CUSTOMER AND OTHER RECORDS: Paper and electronic customer records containing personal data, such as name, signature, physical characteristics or description, address, telephone number, insurance policy number, financial	Operational purposes including service delivery and related business processes	Affiliates and subsidiaries. Third-party service providers (processors) Clients, partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)

Category of Personal Information	Purposes	May be shared with
information, medical information, or health insurance information.		
SENSITIVE, SPECIAL CATEGORY OR PROTECTED CLASSIFICATIONS such as racial/ethnic data, sex, gender, sexual orientation, age, health info, religious beliefs, political beliefs, trade union membership, genetic and biometric data.	Operational purposes including internal management processes, recruitment, service delivery and related business processes	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Clients, partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)
COMMERCIAL INFORMATION including records of products or services considered, purchased or owned.	Operational purposes including service delivery and related business processes	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Clients, partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)
USAGE DATA Internet or other electronic network activity information, such as browsing and search history, and information regarding interaction websites, applications, or advertisements.	Operational purposes including network management, performance analysis and security, account management, service delivery and related business processes	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Clients, partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)
GEOLOCATION DATA Precise geographic location information about a particular individual or device.	Operational purposes including network management, performance analysis and security, data privacy management, service delivery and related business processes	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)

Category of Personal Information	Purposes	May be shared with
AUDIO/VISUAL: Audio, electronic, or visual recordings, or similar information.	Operational purposes including security recruitment and service delivery	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Clients, partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)
EMPLOYMENT HISTORY Professional or employment-related information.	Operational purposes including employee management and recruitment; service delivery inc advertising	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Clients, partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)
EDUCATION INFORMATION	Operational purposes including employee management and recruitment	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Clients, partners, sponsors and other third-party controllers (with consent) Legal authorities (when required by law)
EMPLOYEE DATA Employment-related information that may include the categories above.	Employee management	Affiliates and subsidiaries. Third-party service providers (processors) (with consent) Legal authorities (when required by law)

Sensitive Personal Information

Data privacy legislation typically identifies special categories of Personal Information, which are of greater sensitivity, and enforce additional legal obligations for processing. Sensitive Personal Information may include (depending on the applicable legislation) information regarding:

- Race or ethnic origin
- Political opinions
- Religious or other similar beliefs

- Trade union membership
- Physical or mental health
- Sexual life or sexual orientation
- Criminal allegations, proceedings or convictions
- Genetic information
- Biometric Data
- Financial information
- Official identification information

Where the Processing of Sensitive Personal Information is required, we review risk, establish and record the required lawful conditions for processing (typically explicit consent, employment-related obligation, or other legal obligations) and employ necessary measures to ensure privacy and security.

If such information needs to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected, this will only take place with the explicit consent of the Data Subject.

Transfer and Sharing of Personal Information

It is sometimes necessary to share Personal Information and to transfer it between companies within Amplity Health or to our partners, clients, service providers, and agents. This may also mean the transfer of Personal Information between locations and jurisdictions. In all cases, we apply the core principles above and ensure that the Personal Information for which we are responsible is adequately protected.

- Data Subjects are informed, through appropriate Data Privacy Notices, how we share and transfer their Personal Information.
- Administrative and technical measures are taken to ensure the security of data transfers.
- Appropriate mechanisms and legal instruments are maintained to ensure compliance for the transfer of Personal Information within Amplity Health.
- Third-party agents, suppliers, contractors, and clients are bound by contractual obligation to ensure that the processing of Personal Information complies with this policy and is carried out to an equivalent standard of care.
- Transfers between data privacy jurisdictions are carried out in accordance with applicable legislation and with appropriate safeguards to ensure an equivalent standard of protection. This includes the commitment to applying the principles of the EU-US, EU-UK and Swiss-US data privacy frameworks to all Personal Information received from the European Union, UK and Switzerland (see certification details below).
- Within the limitations set by any applicable law, the Company upholds the rights of Data Subjects to object to, or restrict, the transfer of their Personal Information.
- In certain circumstances, the Company may be required to share Personal Information regardless of the choice stated by Data Subjects. Such circumstances include (i) where required to do so by law or by law enforcement authorities (including compliance with

national security or law enforcement demands) (ii) where, in our opinion, disclosure is necessary to protect the vital interest of the individual (iii) where there is an over-riding contractual obligation (iv) where there are reasons of public interest (v) in order to establish, make or defend a legal claim.

Certification under the EU-US Data Privacy Framework (DPF), the UK extension to the EU-US DPF and the Swiss-US DPF

Amplity Health (specifically Amplity Inc and The Lynx Group LLC) complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce (the"DPF Principles").

- Amplity Health has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF.
- Amplity Health has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF.

If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

The Company's compliance to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

The Company accepts responsibility for the Processing of Personal Information received under the DPF Principles, and accordingly, retains responsibility for Personal Information transferred to third-parties acting as agents on our behalf and shall remain liable if an agent processes such Personal Information in a manner inconsistent with the DPF Principles (unless we prove that we are not responsible for the event giving rise to the damage).

Rights of Data Subjects

The rights of Data Subjects vary across the globe and depend on the relevant data privacy legislation. The Company commits to ensuring that Data Subjects understand their rights under any applicable regime, to providing access to allow those rights to be exercised, and to responding to all legitimate requests in full compliance with the relevant laws. Rights typically include:

1. **Disclosure or Access**:
   - The right to request information about whether and how Personal Information is being processed.
   - The right to be allowed access to that Personal Information and to be provided with a copy in a readily usable and transferable format (portability).
   - The right to obtain the following information: the purpose of the processing; the categories of Personal Information processed; the recipients to whom Personal Information has been disclosed or will be disclosed; the retention period; the source of the Personal Information if not collected directly from the subject and; the existence of any automated decision making based on Personal Information.

2. **Rectification:**
   - The right to allow a data subject to rectify inaccurate Personal Information concerning them.

3. **Erasure ("the right to be forgotten"):**
   - The right to have data erased (subject to certain statutory limitations) and to have confirmation of erasure.

4. **Restriction of Processing:**
   - The right, under certain circumstances, to ask for processing to be restricted.

5. **Objection to processing:**
   - The right to object to the processing of Personal Information (subject to certain statutory limitations).
   - The right to object to disclosure or sale of Personal Information to a third party.
   - The right to object to the use of automated decision making.

Data Subjects are not discriminated against as a result of their choice to exercise their data protection rights.

The Company has put in place, and maintains, SOPs and training programs to ensure adherence to this policy and to support the exercise of the rights of Data Subjects.

Resolution of Disputes

The Company subscribes to an independent dispute resolution mechanism to address unresolved complaints and provide appropriate recourse to Data Subjects, free of charge. As such, we agree to cooperate with, and comply with the advice of, the relevant EU Data Protection Authority, the UK Information Commissioner's Office (ICO) (and the Gibraltar Regulatory Authority (GRA)), or the Swiss Federal Data Protection and Information Commissioner (FDPIC).

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, the Company commits to resolve DPF Principles-related complaints about our collection and use of Personal Information. EU and UK individuals and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact Amplity Health via one of the following channels:

Compliance Hotline	+1-800-344-9100
Email	privacy@amplity.com (emails should be marked 'DATA SUBJECT REQUEST')

This contact information, together with details and contact information for the independent dispute resolution and recourse mechanism must also be made available through appropriate, contextual Data Privacy Notices when Data Subjects are asked to provide Personal Information.

The Company acknowledges and agrees to uphold the Data Subject's right to invoke binding arbitration under certain conditions. Further information may be found here: https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf

Information Security

The Company puts in place appropriate administrative, technical and physical information security measures to support the delivery of this policy and to protect the Personal Information in our care against threats such as loss or theft; unauthorized or inappropriate access, use or disclosure; tampering; loss of data integrity; and improper retention or deletion.

Employees are appropriately trained and expected to take steps to recognize and prevent such threats to Personal Information and to report any suspected or known threat or incident.

Retention of Personal Information

The retention period for Personal Information is determined according to the principle of "storage limitation" as described above: Accordingly, in general, Personal Information is held only as long as necessary for a specified purpose, and the Company takes reasonable steps to minimize the length of time for which that Personal Information is held.

The Company has a "Document Retention and Destruction Use Policy" to define retention periods for certain classes of document in line with statutory requirements. Personal Information contained within these specified document categories is retained on the basis of legal obligation for the stated retention periods. The Company has defined and maintains processes to ensure that Personal Information is anonymized (de-identified) or safely deleted in line with the principle of storage limitation and the Document Retention and Destruction Use Policy.

Marketing and Promotional Activities

The Company does not typically engage in marketing and promotional activities targeted at individuals or consumers for its own purposes, but may do so on behalf of our clients. In all cases, the Company complies with applicable law and ensures that the rules of consent are implemented and that the rights of the individual or consumer are upheld.

Administration and Compliance

The Company maintains a Data Privacy Management System to ensure robust governance of data privacy. This includes:

- Adoption of this Policy and definition of compliant practices.
- Documentation of the implementation of the required administrative, organizational, and technical measures.
- Analysis and documentation of data privacy risks and impacts.
- Recording of processing activities to demonstrate and monitor compliance.
- Recording, investigation, and reporting (where required) of data privacy breaches.

The Company appoints a Data Privacy Officer (DPO) to advise on data protection obligations and the implementation of necessary compliance measures, to monitor internal compliance and to act as a first point of contact for data subjects and the relevant supervisory authorities. The DPO is independent and reports to the top level of management, and is adequately supported and resourced.

Expectations and Training

The protection of Personal Information and compliance is the responsibility of all employees and others working on our behalf.

The Company ensures appropriate training to support its employees in the delivery of this policy.

Any potential or perceived violation of the principles outlined in this policy must be immediately reported to the Corporate Compliance department.

Terms and Definitions

Term	Description
Company	Amplity Health, comprising Amplity Inc, Amplity Ltd, Lynx Group LLC and other affiliated entities
Controller	A Controller determines the purpose and means of processing Personal Information.
Data Subject	An identified or identifiable individual (otherwise described in different legislation as a “natural person,” “consumer” or similar term) whose Personal Information we Control or Process.
Personal Information (or Personal Data)	Information that relates to is capable of being associated with or can be linked to a Data Subject, both directly or indirectly. Personal Information is to be considered as belonging to the Data Subject.
Processing (of Personal Information)	Any operation performed on Personal Information, such as collection, storage, organization, adaptation or alteration, retrieval, use, transmission or transfer of Personal Information for a lawful purpose.
Processor	A processor is responsible for Processing Personal Information.

Approvals

POLICY APPROVER

Name Eric Green Signature _____

Title General Counsel Date 28/2/24

Versioning

Version	Effective Date	Change History
V1	3/18/2020	• Initial Draft
V2	3/1/2022	• Review / minor corrections

V3	28/2/2024	• Update to include EU-US DPF inc UK extension & Swiss-US DPF
		•
		•
		•
		•