# Global Health Alliance
# Information Privacy Policy

**Policy Date: 4/29/2025**

**Project Manager: Anonymous**

**Project Team: Group A**

## Table of Contents

# A. Overview

## *Introduction*

Since the onset of the modern digital age, the protection of personally identifiable information (PII) has been both a legal and ethical imperative, especially in regards to organizations that operate across multiple international regions and handle sensitive data such as medical information. As a prominent medical institution with not only a global footprint in Europe, but also several offices in the United States, our organization understands the importance of managing and protecting PII of patients as well as strives to implement a privacy policy that embodies such.

In this privacy policy, our goal is to clearly define how Global Health Alliance (GHA) will collect, store, use, and protect PII as well as where individuals within our organization will fit in within the security governance framework and their corresponding roles and responsibilities. Given GHA is headquartered in San Francisco with widespread locations in both the United States and Europe, we aim for our policy to align with the various unique regulatory standards in both regions including state-level legislation within the United States as well as higher overarching statutes of the European Union. Our organization will adhere earnestly to this policy and demonstrate our commitment to safeguarding PII during all states of data.

## *Rationale for Policy*

Our rationale behind this policy was based on ensuring compliance with all types of data protection laws regardless of region, tailoring protection to individual rights, and establishing a uniform approach for PII management in a global institution. This was especially vital for us because the healthcare sector already naturally involves data-intensive procedures with sensitive information and is also largely dependent on a foundation of trust that such information is protected. At our organization, we seek to employ industry standard practices in data governance and protection to better secure and support healthcare providers, staff, and patients which will inherently lead to better performance and results.

Our privacy policy's first established baseline is that compliance with regulations such as the European General Data Protection Regulation (GDPR), federal decrees in the U.S. including the Privacy Act, and even state-level laws like the California Consumer Privacy Act (CCPA) is an obligation and not optional. By following these standards, our organization will impose strict procedures for handling PII including requirements for consent, access controls, breach notifications, and more. Ultimately, taking the time to develop a comprehensive privacy policy framework will also reap more long-term benefits by avoiding potential financial penalties and reputational damage. Aside from regulatory compliance, another aspect of forming a robust privacy policy was to help with protecting the rights and interests of various individuals that will be interacting with our institution including staff, customers, business partners, and other stakeholders. As emphasized earlier in this section, medical institutions such as ours, by nature, handle

especially sensitive PII like health records, medical history, contact information, identification numbers, and insurance information. As such, it was our utmost priority to devise a privacy policy addressing both cybersecurity risks such as data breaches and unauthorized digital access as well as general security risks on a broader scale.

## *Laws and Regulations*

GDPR (General Data Protection Regulation):

The GDPR is a data privacy and security law in the European Union (EU). It is considered to be one of the toughest data protection policies to exist. Those that violate the GDPR are penalized with large fines. The GDPR places restrictions not only on data controllers and processors, but also any business that has personal data of people in the EU regardless of if those businesses are based in the EU or not. It places guidelines on what data is allowed to be collected and processed, how that data is to be processed, how consent is defined, and whether the business will require a data protection officer. The GDPR focuses on protecting personally identifiable information, including health information, using the following seven principles:

- Lawfulness, fairness, and transparency: The processing of data has to be lawful, fair, and transparent to the data subject. In healthcare, this includes having a legal reason for collection and informing the data subject that their information, such as name, date of birth, and medical history, is being collected.

- Purpose limitation: Data can only be processed for specific purposes that the data subject is made aware of at the time of collection. This can include information such as medical history and family history, but exclude things such as music interests and phone call history.

- Data minimization: Only the necessary amount of data needed for the specific purpose should be collected and processed. If a patient is being checked into the hospital, the institution should provide medical history, current medications, and allergies, but not a detailed family history that is irrelevant to the patient's condition.

- Accuracy: The data collected and processed should be both accurate and up to date. If a patient is misdiagnosed, the data should be corrected and updated as soon as possible.

- Storage limitation: Data collected and processed should only be stored for as long as necessary for the purpose. For example, pediatric records may no longer be relevant for a patient that is 80 years of age, and thus should no longer be stored.

- Integrity and confidentiality: The processing of data should include measures that ensure that the data is secure, maintains its integrity, and is confidential. Under healthcare, this involves ensuring that patient information is not manipulated or shared with anyone unauthorized.

- Accountability: Data controllers have to be able to show that they are compliant with the GDPR. In the healthcare setting, this can look like establishing a data protection officer that advises, audits, and monitors the collection and processing of data to make sure the medical institution is GDPR compliant.

The GDPR also establishes privacy rights that provide data subjects with more control over their personal data. The privacy rights are as follows:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

HIPAA (Health Insurance Portability and Accountability Act):

HIPAA is a U.S. law that establishes federal standards protecting sensitive health information from disclosure without the patient's consent. It covers healthcare providers, health plants, and healthcare clearinghouses, and associated businesses. Its goals are to provide continued health insurance coverage to those that may be unemployed and to standardize how administrative and financial information is shared electronically. It contains five titles, the most relevant to this medical institution is Title II, specifically the HIPAA privacy rule under Title II. This rule protects a patient's health information in any transmittable format by limiting when a patient's health information can be disclosed without proper authorization. It also enforces the development of privacy policies, a privacy personnel, workforce training and management, mitigation, safeguards, the ability for data subjects to lodge a complaint, the institution's inability to retaliate, and documentation and record retention.

HITECH (Health Information Technology for Economic and Clinical Health Act):

The HITECH Act strengthens HIPAA and the protections granted under that by expanding the laws surrounding health information that is electronically protected. It also defines what a breach is and how breaches should be notified to affected individuals. It states that in the case of a breach, affected individuals should be notified within 60 days via email, and the department of Health and Human Services and proper media should be notified if the breach affects more than 500 individuals. The HITECH Act also incentivizes healthcare providers to switch to electronic health records. It mentions technologies, such as encryption and data destruction, which aids in the

protection of information. Data destruction is described as involving media sanitization, clearing, purging, and destroying.

CMIA (Confidentiality of Medical Information Act):

The CMIA is a California law that expands HIPAA and focuses on healthcare providers, healthcare plans, contractors, and at times pharmaceutical companies. In order for healthcare providers to release medical information, they must first get the proper, written authorization. Healthcare providers must also create, maintain, store, or destroy medical information in a way that would maintain the confidentiality of the information. While the CMIA focuses on protecting the privacy of medical information, it also describes when medical information can be disclosed. If a patient wishes to see their information, they must be able to within a reasonable timeframe of 5-15 days. Patients are able to send in an addendum which notes any incorrect information and its respective changes. This addendum must be included in the patient's record. The CMIA awards damages to those who have had their privacy violated, as well as fines for entities that are not CMIA compliant.

CCPA (California Consumer Privacy Act):

The CCPA grants consumers, including patients, with control over collected information. Consumers can ask to know where their information is being collected from, why it is being collected, and what third-parties it is shared with. Consumers are able to delete their personal information and opt-out of the sharing of their information. The CCPA applies to healthcare organizations and health information that are not included under HIPAA or CMIA. One such information could be financial information. Financial information does not fall under HIPAA or the CMIA, but may be collected by healthcare providers. Thus, it is important that medical institutions remain compliant with CCPA.

CPRA (California Privacy Rights Act):

The CPRA is a California law that expands the CCPA. It includes additional rights that consumers have, such as the right to fix wrong information, the right to know about and opt out of automated decision making, and the right to limit the use of sensitive information. It also rewrote some of the rights under the CCPA, such as the right to data portability and the right of minors. The CPRA also redefined sensitive information to include more categories of information. It created the California Privacy Protection Agency which is under the authority of the California Attorney General. The California Privacy Protection Agency ensures and certifies that businesses are compliant with the CPRA. The CPRA increased the fines of violations.

## *FIPPs*

Organizations, including medical institutions, are recommended to abide by the Fair Information Practice Principles when evaluating things that can affect privacy. The principles are a guideline that organizations can use when developing their privacy plan. The principles are as follows:

- Transparency: Transparency is the idea that information regarding the institution's privacy policies, such as how they collect, process, share, and store it, should be readily available. Anyone who wants to know this information should be able to easily find it. In a medical institution, this can look like posting a detailed privacy policy on their website.

- Individual Participation: This consists of involving the data subject whenever possible in the data collection and processing steps. This can include things like asking them for consent, and allowing them to alter or delete information. It can also look like establishing a system in which individuals can lodge complaints and ask questions. In the healthcare setting, it could look like making sure the patient consents to having their information recorded and allowing them access to the data if they want to correct a mistake a physician may have made. It can also involve adding a questions or concerns box on the institution's website.

- Authority: Under the principle of authority, businesses should only collect and process data that is necessary and relevant to a specified purpose. Their authority should be identified and noted. This could mean a nurse writing down a patient's information, such as date of birth, name, and current medications, and then signing off on the paper.

- Purpose Specification and Use Limitation: Data subjects should be aware of why their data is being collected, and only the data for that notified purpose should be collected. For example, medical institutions should inform patients that information regarding their current medications are being collected to ensure that any additional medication provided, does not interfere with them.

- Minimization: The minimization principle states that only relevant and necessary information should be handled in the time needed to complete the purpose. This means that if a patient is admitted for a broken leg, unrelated family history should not be collected, and other information should only be stored until the leg has been healed.

- Quality and Integrity: This principle maintains that data collected should be complete, correct, relevant, and timely. In a medical institution, this can mean updating a patient's chart if they have been misdiagnosed.

- Access and Amendment: Data subjects should be able to request to correct or alter their information. For instance, in a healthcare scenario, if a patient sees that they are listed as having a latex allergy, when they actually do not have one, they should be able to send in a request to remove that allergy.

- Security: Institutions should implement safeguards, proportional to the projected risks, that will protect sensitive information. These safeguards should be administrative, technical, and physical. It should protect data from unauthorized access, unapproved alteration or destruction, and misuse. Medical institutions can hire a chief privacy officer, implement role-based access, and monitor server rooms.

- Accountability: Institutions should be held responsible for compliance with the laws and principles. They should also train their employees so that they are aware of the policies and hold them accountable if they are ever not compliant. Medical institutions can perform audits every quarter and hold training seminars for new employees and whenever there are new policy changes. Hosting refresher training seminars for current employees can also be helpful.

# B. People, Risks, and Responsibilities

## *Policy Scope*

To ensure complete privacy of patient data, this privacy policy applies to all individuals providing paid or unpaid services to Global Health Alliance. This includes employees (full-time, part-time, and contractor), interns, volunteers, and third-party service providers across all global offices in the US and Europe. This privacy policy applies to all departments within the organization, including Clinical, Research, IT, Administrative, and Marketing.

This policy covers the collection, use, storage, and protection of patients' Personally Identifiable Information (PII) and Protected Health Information (PHI) in digital and physical formats.

PII is data that can be used to identify an individual. For the scope of this policy, it includes the following:

- Basic identity data (Full names, date of birth, gender, biometrics)
- Contact information (Address, phone number, email address)
- Identification numbers (SSN, driver's license, passport number, work ID, school ID)
- Digital identifiers (Login credentials, IP address)
- Any personal information that is linked or linkable to one of the above

PHI is health-related data that can be used to identify an individual and for the purpose of this policy it includes:

- Medical history and records (Diagnoses, conditions, and treatment plans)
- Clinical records (Lab results, prescriptions, doctor's notes)
- Appointment records (Date and time of appointment, type of care received)
- Health insurance information (Policy numbers, claims, and billing information)
- Any personal information that is linked or linkable to one of the above

## *Data Protection Risks*

In the IT field, risk refers to the chance that an event could cause harm or disruption, based on how serious the impact would be and how likely it is to happen. It is crucial to risks that could harm the organization in advance, especially since new forms of malware and hacking are being developed constantly.

Examples of data protection risks include:

- Usage of outdated/legacy systems: Systems not being patched daily are more susceptible to breaches and hacking. A company with stakeholders needs to adopt technology that is actively being maintained.
- Identity theft: A victim being impersonated by a malicious actor can access organizations' files once they successfully steal an identity.
- Ransomware: Malware that encrypts a victim's data where the attacker demands a "ransom", or payment, to restore access to files and network.
- Internal employees, contractors, vendors, etc.: Employee misuse or inappropriate access of data, unintentionally or intentionally
- DDos Attack: A distributed denial of service attack where the site is overwhelmed with traffic, such that authorized users are unable to access the site.
- Phishing: A hacker manipulates someone into revealing sensitive data. They lure the person in by pretending to be a legitimate friend, colleague, or professional.
- Physical theft: Some examples of physical theft may be stolen laptops and documents.
- Unauthorized access: Unauthorized access (including breaches, shared login credentials, etc.) to sensitive medical information.
- Insufficient data destruction: Data is destroyed improperly when it is no longer needed.
- Data loss: Permanent or temporary loss of sensitive patient data due to accidental deletion, hardware failure, or corrupted systems.
- Misconfiguration in systems/devices: For example, Open ports, unchanged default configurations.
- Inaccurate/false information: Human error (User/Employee) and intentional changes made by malicious actors can lead to inaccurate/false information.
- Use of unapproved devices: Staff use personal devices or apps without approval.
- Overcollection of patient data: Gathering more personal or medical information than is necessary, increasing exposure risk.

- Third-party vendor breaches: A partner or software vendor suffers a breach affecting your data.
- Unencrypted communication: PHI might be sent over unencrypted emails or texts.
- DDOS attack: A distributed denial of service attack where the site is overwhelmed with traffic, such that authorized users are unable to access the site.
- Misuse of data: Misuse of patient data for marketing purposes.

## *Responsibilities*

### 1. Regulatory Compliance

- Adhering to HIPAA for protecting patient health information (PHI) in the U.S.
- Complying with CCPA/CPRA for California residents' data rights.
- Ensuring GDPR compliance for processing personal data of EU citizens, including appointment of a Data Protection Officer (DPO) and observance of cross-border data transfer requirements.
- Compiling with HITECH (Health Information Technology for Economic and Clinical Health Act), which strengthens HIPAA.
- Complying with CMIA (Confidentiality of Medical Information Act), which is a California law that expands HIPAA.

### 2. Data Security

- Implementing appropriate technical and organizational safeguards to secure data.
- Conducting regular risk assessments and system audits.
- Preventing unauthorized access, disclosure, and data breaches.

### 3. Transparency and Communication

- Clearly informing individuals about what data is collected, how it is used, and their rights.
- Publishing and maintaining accessible and up-to-date privacy notices.

### 4. Consent and Individual Rights

- Obtaining explicit consent where required (especially under GDPR).
- Supporting rights to access, correct, delete, or transfer personal information

**5. International Data Transfers**

- Utilizing approved legal mechanisms (e.g., SCCs, BCRs) for transferring data between the U.S. and Europe.

**6. Third-Party and Vendor Oversight**

- Executing Business Associate Agreements (BAAs) and ensuring all partners comply with relevant privacy laws.
- Monitoring vendors for ongoing data protection compliance.

**7. Employee Training**

- Providing regular, role-based privacy and security training.
- Promoting a culture of compliance and awareness throughout the organization.
- Ensure employees do not use unapproved devices, overcollect patient data, or misuse data.

**8. Incident Response**

- Maintaining a structured breach response plan.
- Ensuring timely notification to affected individuals and regulatory authorities in the event of a data breach.

## *General Staff Guidelines*

The following are brief guidelines on how all staff should uphold the privacy and security of patient data within the organization (more detailed information will be provided in future privacy awareness programs):

1. All staff must comply with role-based access control mechanisms: Global Health Alliance will provide staff with access to patient information based on a needs-basis.
2. All staff must maintain patient confidentiality in and out of the office: Discussing patient information in public spaces will not be tolerated. Also, physical or digital files containing patient information should never be left unattended or open on shared computers.
3. Staff must use company-approved systems when dealing with patient data: Global Health Alliance will provide staff with necessary hardware (laptops, mobile

devices, etc.) and software (VPNs, encrypted tools, etc.) to complete their work responsibilities. Personnel should never use their personal devices or software to complete their job responsibilities.

4. Staff are expected to practice data minimization: Staff engaged with patient data collection should only collect the minimum amount of PII or PHI from patients in order to conduct clinical, marketing, or operational responsibilities.
5. Staff are expected to attend annual privacy and security training programs: All employees are required to complete annual privacy training (courses and seminars) to stay up to date on organizational privacy protocols.
6. Staff must report privacy incidents promptly: Immediately report any data breaches, suspected breaches, or suspicious activity to the privacy team.

# C. Requirements for PII

## *Data Storage*

This section details the methods that will be used to protect stored PII. Having various security measures and backups will mitigate the potential security risks that could threaten our organization.

- Encryption
    - Encryption is a way to protect data by encrypting data, making it unreadable, unless the user has the proper key/authorization to unlock the encrypted data.
- On-Site Backup Storage
    - This kind of backup storage is physically stored on-site on a server as a way to retrieve data in any kind of emergency situation. Only authorized employees are able to access the physical location and the data stored.
- Off-Site Backup Storage
    - Similar to the on-site backup storage, however this server will be stored off-site. Somewhere physically separate from the operating site. This method will be used to retrieve data in case the on-site backup storage cannot be accessed.
- Cloud Backup Storage
    - This kind of backup is still stored on a physical server however the data will be uploaded through a third party service using the cloud as a way to remotely store data.

- Access Control
    - This method is about having only authorized individuals to access the minimum amount of data. Access control will be given depending on their role in the organization.

## *Data Use*

This section details the methods that will be used to protect PII in use. Data in use is more fluid, meaning the data is being used and shared by various users. Proper measures have to be set in place for data in use as to not have it fall in the wrong hands.

- Encryption: Like data storage, encryption works well for data in use. As the data is encrypted to those who do not have proper access to the data. Only the authorized users sending and receiving the data may view the data unencrypted.
- Data Sharing: To prevent data being shared with unauthorized parties, data must be shared only with authorized users and/or parties.
- Multi-Factor Authentication (MFA): MFA makes it so that when a user tries to access data through normal credentials, a second verification is required to proceed. The most common form of verification is using a secondary device, like a phone, to receive a request that confirms the user is the one logging into the service.
- Data Anonymization: This method hides certain pieces of data about someone to make them less identifiable. This could be used in a way where higher level individuals can see more data the more access they have.
- Nonrepudiation: Makes sure that data sent by users/parties cannot be denied and is verified using encryption and digital signatures embedded within the data being sent.

## *Data Accuracy*

Inaccurate or outdated patient information can compromise patient safety and institutional reliability. For instance, inaccurate logging of a patient's symptoms in their medical records can lead to them being prescribed the wrong medications. On the other hand, outdated patient information can prevent patients from receiving appropriate care.

To maintain trust, compliance, informed decision-making, and high-quality care, all staff are responsible for ensuring that patient PII and PHI are up to date. The following data accuracy guidelines should be followed by employees:

1. Initial Verification: Verify PII/PHI for accuracy at the point of entry into the organization's system. This includes confirming spelling, contact details, and identification numbers directly with the patient whenever possible

2. Ongoing Updates: Staff should correct any mistakes or outdated information in collected PII/PHI swiftly and proactively. When patients return to the office after more than 6 months of care, they should be asked if they would like to make any updates to their personal or health data.

3. Data Update Procedures: Employees responsible for updating patient data should follow data update procedures outlined by the organization. This includes creating proper documentation of data changes in order to maintain data integrity and proper audit trails.

4. Data Subject Rights: In order to be compliant with regulations like HIPAA and GDPR, data subjects (patients) will be given the opportunity to review their PII and request any corrections. Staff are expected to support these patient requests in a timely and respectful manner.

# D. The External Context

## *PII Principal Requests*

Global Health Alliance is committed to the protection and upholding of rights belonging to all individuals whose data we process, otherwise known as PII principals. We firmly believe that these individuals are entitled to legal and ethical rights in regards to any personal data we may need to collect, process, use, and store. This section involves outlining mechanisms for PII principals under our organization to understand and exercise their rights, be aware of procedures for processing their requests, and have faith in our organization's dedication to transparency and accountability.

PII principals at our institution will have the right to:

1. No data surveillance/spying without cause
2. Prevent groups and third parties from using their data without permission
3. Hold those who steal and/or misuse their data accountable
4. Maintain social and data collection boundaries
5. Protection of private and personal data
6. Control their own data and the way it is used
7. Free speech and thought without fear of being monitored
8. Engage freely with politics without fear of exposure and/or consequences
9. "Be forgotten" and remove private information at risk for causing reputational damage
10. Protection of financial information from threats of theft, unauthorized disclosure, etc.

These rights can also be found under various international and domestic laws and regulations including the GDPR in the EU, the CCPA in the U.S., and the FIPPs. By creating policies and procedures in line with such standards, our organization aims to facilitate a culture of respect and professionalism extending beyond base compliance.

To further support PII principals in exercising their rights, Global Health Alliance developed base key procedures for submitting PII requests:

- Submitting requests: Global Health Alliance offers multiple submission methods including secure online forms through our website, email, physical mail, or even in person at our offices. To supplement, we require verification of identity as an additional layer of security.

- Verification: When verifying one's identity, Global Health Alliance will need verifiable information prior to processing any PII request. Additional documentation (birth certificate, SSN, passport, etc.) may be required.
- Timeline: Global Health Alliance's target response time is to provide an initial response to PII requests within seven calendar days and fully resolved in about a month, the typical recommendation by GDPR Article 12 and CCPA Section 1798.130.
- Follow-ups: In Global Health Alliance's responses, requesters will be informed of the outcome as well as, in the case of a partial or full rejection to a request for data removal, contingent reasonings (i.e. required by law to retain data). Communications are mandated to be transparent and accessible in order to properly guide PII principals through procedures.

Finally, Global Health Alliance pursues continuous learning and improvement in all operational aspects. We adhere to a regular schedule of auditing PII request procedures for functional and compliance reasons to match the evolving legislations and stakeholder needs. Global Health Alliance encourages PII principals to speak out and provide any feedback on regulatory, social, and ethical issues. By fostering open dialogue and consistent assessments, we aspire to garner trust and fulfill the responsibilities of guarding personal information.

## *Disclosing Data*

Our organization follows strict, well-defined protocols when it comes to the disclosure of personally identifiable information. We view the release of such data as a serious matter that must be approached with purpose and precision. Disclosure occurs only under specific and justified conditions: when required by law, when necessary to fulfill obligations, or when the PII principal has given consent.

When required by law to disclose information we comply fully, but we also ensure that such requests are valid and appropriate. Disclosures are reviewed by legal personnel to confirm that the organization is meeting its responsibilities while minimizing unnecessary exposure of sensitive data. In emergency scenarios, where disclosure may be necessary to protect someone's life, health, or safety, the organization still applies principles of minimization and documentation to ensure that information is shared responsibly.

Beyond legal requirements, disclosures may be necessary to work with third-party vendors, auditors, or contractual partners. Recipients are required to sign formal agreements affirming their adherence to our organization's privacy standards. These agreements include clauses ensuring compliance with different laws depending on the jurisdiction.

Every instance of disclosure is also documented. These records include the nature and sensitivity level of the data shared, the party or parties to whom it was disclosed, the justification for disclosure, and the method of transmission. All disclosures must occur

through secure channels such as encrypted digital platforms or secure APIs. We also maintain a regular review process to evaluate disclosure activities, ensuring they remain compliant with the law, effective in purpose, and respectful of individual rights. Our goal is not simply to comply with legal standards, but to exceed them, reflecting our belief in ethical collection of personal data.

## *Providing Information*

Global Health Alliance believes that providing clear and accessible information about how we collect, use, and share personal data is not just a requirement, but a fundamental principle of how we want to run our company. Every PII principal has the right to understand how their data is handled, and we are committed to ensuring this through transparent communication. At the time of data collection, individuals are provided with a comprehensive privacy notice that outlines all relevant details in plain, understandable language. This includes what categories of personal information are collected, the specific purposes for which the data will be used, the duration for which it will be retained, and the parties with whom it may be shared. We also describe the legal basis for data processing, along with the rights available to the data, such as access, correction, and deletion.

The notice is made permanently available on our organization’s website and is updated whenever there are changes made. Our privacy team is available on standby to help PII principals understand their rights and our practices through customer support. This organization affirms its dedication to the principles of transparency and respect.

## H. Executive Sign-Off

| Name | Title | Signature | Date |
|---|---|---|---|
| Anonymous | Chief Executive Officer | *Anonymous* | 4/29/2025 |
| Anonymous | Chief Financial Officer | *Anonymous* | 4/29/2025 |
| Anonymous | Chief Information Officer | *Anonymous* | 4/29/2025 |
| Anonymous | Chief Marketing Officer | *Anonymous* | 4/29/2025 |
| Anonymous | Chief Information Security Officer | *Anonymous* | 4/29/2025 |
| Consin Hu | Chief Privacy Officer | *Consin Hu* | 4/29/2025 |

*The signatures of the people above relay an understanding of the purpose and content of this document by those signing it. By signing this document, you agree to this as the Information Privacy Policy.*