We have built Thereafter from the ground up with an emphasis on security. Author Data contains the most important, most personal, and most valuable data of our users. Securing Author Data is a collaborative effort between Thereafter and our users. We are committed to providing detailed explanations of our security measures – explaining how we secure data and what we do to verify those methods. This will serve to educate users and provide them confidence. Transparency in this regard will help us ensure we continue to deploy best in class security throughout all aspects of our platform. Everyone at Thereafter is committed to maintaining an absolute zero-fail approach to data security. Security has been a fundamental consideration at all phases of our initial platform development, and it will remain so. Security is an ongoing effort, so we are continuously working to maintain and improve it.

Our focus on security begins immediately upon user account creation. When creating an account, users are prompted to create a password or passphrase to pair with their email address/username. Next, users will select their preferred method for their second factor of authentication – user passwords/passphrases will be paired with a one-time code delivered via authenticator app, SMS, or email. Requiring additional protection for the login process creates defense in depth, ensuring security of user accounts and Author Data.

Users must create passwords more than 10 characters in length, containing at least upper- and lower-case characters. Users should create a password which is unique to Therafter, and not be something that has been used previously. We strongly recommend users utilize a password manager or create a passphrase. This will pair a unique, high entropy password with the additional authentication, helping us to protect every user's account.

Thereafter does not store user passwords or any information which could enable an attacker to obtain user passwords. The password itself is not stored within our servers, as we utilize the Secure Remote Password (SRP) protocol. This protects authentication from brute force and man in the middle attacks. This also places a high level of importance on users remembering and/or ensuring access to their password.

Thereafter does not retain your login credentials in any form, and we will never request you to provide them to us. We urge users to be especially vigilant in protecting both their password and additional authentication method. If users utilize a password manager to create or store a password, they should ensure access to that password manager from multiple devices. Users will be provided the option of either requiring the second factor authentication with every logon or trusting their device for 15 days. This is provided for convenience, but we urge users to consider both options, and choose one which makes sense for their expected usage, location, and security of their device.

Now that a user has an account with Thereafter, created a strong password, and selected their second factor authentication method, they are ready to begin storing and creating Author Data within their enclave. Maintaining security of Author Data while ensuring it is always available to the user and their designated connections, when the time comes, is the

primary function of Therafter's platform. To accomplish this, our platform does three things: 1. Ensure a user is properly authenticated before providing access to their Author Data, 2. Maintain the confidentiality and integrity of that data 3. Deliver each data element to its intended recipient at the designated time.

Item 1, authentication was covered in the first section, leading us to item 2: confidentiality and integrity of Author Data. This involves two fundamental aspects. Author Data must be protected in storage, between instances when a user accesses it, known as "data at rest". Author Data must be securely transmitted to a user when they access it, known as "data in transit".

How is Author Data protected at rest? Author Data is stored safely within Thereafter's AWS based platform. Thereafter's platform, and all Author Data, is hosted in servers in the US. Within the platform, Author Data is encrypted using the Federal Information Processing Standard (FIPS) approved Advanced Encryption Standard (AES-256). Author Data is encrypted with a 128 bit Secret Key, only accessible to the user, combined with the user's password. This ensures user data is only ever accessible by that user, or their designated recipient(s) at their specified time(s). It also means that each user must be sure to adequately protect and maintain access to their keys.

How is Author Data protected in transit? Author Data is transmitted using the latest secure protocol. Transport Layer Security (TLS) version 1.3 utilizes the latest and most secure cryptographic cipher suites. Version 1.3 provides this security while minimizing time required to complete a successful handshake. Utilizing unique session keys for each transaction (perfect forward secrecy) prevents an attacker from compromising future exchanges by obtaining any individual key. This ensures that when a user access their Author Data, it is delivered to them, only to them, and it is available upon their request.

After creating and storing their Author Data, a user must designate a verifier and add connections who will be designated to receive individual journal items or Author Data elements.

A user has now created their account, stored their Author Data, selected a verifier and added connections. Thereafter is committed to maintaining the integrity and security of Author Data for an extended period of time (subject to account status and other Terms/Conditions) in order to facilitate the delivery of that Author Data to connections upon the user's passing. In support of this effort, we urge users to make sure their connections are current and a recipient is designated for all Author Data entered into the platform. Since we will not have any access to your data, we will have no way to deliver it in the event you do not designate a recipient.

A user's password, encryption key, and all Author Data belongs to the user. All Author Data will only ever be viewable by the user, or their intended recipients at the time of their passing. Thereafter does not receive or retain unencrypted data and does not have a way to

access that data. Maintaining absolute security of this data is fundamental to our operation and is the primary driver of the other aspects of our security focus (encryption of data at rest and in transit, secure authentication, and third-party analysis of our platform). Thereafter is not able to alter the recipient or timed release of Author Data, so we urge users to designate these items accordingly as soon as they are added. Users must also be sure to keep their recipients current, and follow up with recipients to ensure they have confirmed their own access to the platform. Thereafter's guarantee that Author Data belongs only to the user necessitates this. We do not have any access to any part of a user's Secure Data. This extends to designated recipients in addition to the data itself. Thereafter will not be able to verify, or correct after the fact, outdated contact information for a recipient.

Thereafter does not have access to, and cannot provide access to, a user's Author Data. Because of this, we strongly recommend users securely retain their login information through a means that ensures availability. Thereafter cannot decrypt your Author Data should you lose or forget your login credentials. Because of this, we advise users to retain their login credentials either within a secure password manager or in a safe, accessible, offline location. Since Author Data is, and remains property of the user, we provide the option of requesting a full export of your Author Data from within the platform after you have logged in. If a user decides to end their subscription, they will be provided sufficient time to login and retrieve their Author Data. If you end your subscription, or your Author Data has been disseminated to all intended recipients following your passing, Thereafter will securely and irretrievably delete your data from the platform.

Service data, separate from Author Data will be acquired during your usage of the platform. Service Data includes but is not limited to: server logs, billing information, usage information, email addresses. While you are using our services, we retain the right to hold and use this service data to provide our services, and this service data is kept confidential. We do not sell or rent any of your personal information to third parties. Service data might be shared with our service providers.

As we have developed our platform, addressing security at each phase of the user experience, we also recognize the ongoing need to improve our security as technology advances and best practices evolve. With the goal of verifying our current posture and identifying future improvements, we have engaged an industry leading information security firm to provide an independent assessment of our initial platform. We also plan to conduct regular recurring assessments, addressing any identified issues proactively. A letter of attestation provided following their assessment of our launch platform can be accessed on our website. In addition to penetration testing and security assessments, they are engaged in research and education efforts through multiple organizations (SANS, Black Hat, and others). This forward looking approach will help Thereafter identify and deploy platform enhancements as our user base grows and technology advances.

Thereafter is committed to continuing to advance our security posture in accordance with advancing technology or emerging vulnerabilities. We plan to stay on the forefront of security advancements, so we are not playing catch up when legacy protocols or algorithms are deprecated, or vulnerabilities are discovered. Some of these advancements may require user participation – since Thereafter cannot access your data, we cannot enhance its encryption, for example. We expect security and our roadmap of future security enhancements to be an ongoing discussion with users as out platform advances.

We look forward to sharing more about these enhancements as they are identified and we schedule their implementation, but they will include things like: implementing passkeys for login and Secure Data sharing with connections, implementing post quantum encryption (FIPS 203), or future updates to the TLS protocol. While we intend to be on the forefront of these advancements, providing best in class security to our users, we are not going to use our platform as a test-bed for emerging technologies. We will aggressively implement enhancements early, but only when they are proven. This page will continue to be updated so that it remains current, and we encourage users to reach out with any questions they might have about the security of their data which have not been addressed by this outline.