PROGYNY PRIVACY, INTEGRITY, AND SECURITY

At Progyny (“we,” “us”), we take ensuring the security and privacy of our members' sensitive information seriously. The following summarizes some of the key elements of our information security and privacy programs as well as some of the measures we have implemented to increase the privacy and security of the member information we store.

Data Collection & Privacy Compliance

We only collect and retain the minimum necessary data provided from our members to provide our fertility benefits administration services. For further details regarding the kind of data necessary for us to provide our services and how we utilize it, please review our privacy policy: https://progyny.com/Privacy-policy/

We ensure that the member data we collect resides in technical environments that utilize industry best-practices for data protection. This helps maintain the data’s integrity, security, confidentiality and works to prevent unauthorized access.

While we are providing services to members, we are committed to ensuring that the data we collect is accurate, up to date and complete. We will check in with our members to identify changes and make updates to the information we have on file. Through the use of our app, members can also ensure the information we have on record remains accurate and true.

We maintain a dedicated privacy team that is tasked with ensuring continued data privacy compliance following applicable rules and regulations. The privacy team works in parallel with our information security team to ensure there are industry-standard technical and administrative measures in place to protect all member data.

We require all Progyny personnel to review and complete privacy and security trainings annually on Progyny’s privacy and securities policies, practices, and applicable laws.

Information Security Management

We regularly conduct risk assessments of our information security environment, following the National Institute of Standards and Technology (NIST) Risk Management Framework. This process enables us to identify and address potential vulnerabilities and threats effectively. Identified risks are tracked in our risk register, where we can assign impact and likelihood and assign relevant teams to plan methods to address found risks.

We recognize the need for continuous improvement in our information security management system, and as such, we establish annual targets and objectives to develop and enhance our security program. These are based on the outcomes of our risk assessments, as well as the latest industry best practices and emerging technologies.

To date Progyny has not experienced any major incidents involving member data, we track and remediate issues as identified to investigate what occurred and if applicable prepare a response. Our incident management program is designed to quickly and effectively respond, remediate, and learn from such events. This approach involves collaboration among our IT, engineering, security, and operational

teams, ensuring that all aspects of an incident are addressed and resolved in a timely manner. We leverage a suite of tools to regularly monitor and detect any events that require a response.

To further ensure the effectiveness and robustness of our security program, we engage reputable third-party organizations to audit our existing practices and provide recommendations for improvement. These external evaluations allow us to maintain a high level of transparency and foster a culture of continuous learning and development. These evaluations include annual penetration tests, at least quarterly vulnerability scans, and annual controls testing.

Our commitment to security extends to third-party vendors who may handle sensitive member data or provide services on our behalf. We conduct reviews prior to contracting and during onboarding that identify risk exposure by the vendor. We also perform ongoing evaluations to ensure continued adherence to our security standards. These reviews are facilitated using OneTrust, a platform that automatically collects relevant security documentation and third-party environment assessments. Appropriate security agreements may also be incorporated into master service agreements with vendors before they process sensitive data on Progyny's behalf.

Business Continuity Management

Progyny maintains a business continuity program, which is continually improved and updated to encompass both existing and new services deemed vital to our operations. We establish annual targets and objectives to develop and enhance our business continuity program. Additionally, we assess the criticality of core services in order to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to acceptable levels. The program comprises daily backups of critical systems and consistent testing to guarantee rapid service restoration in case of an outage. Our engineering and IT teams are well-trained in recovery procedures, while service-providing staff members are trained in utilizing our disaster recovery networking services.

We actively monitor our program and document areas where improvements can be made to our response, ensuring that the business continuity plan remains relevant, adaptive, and effective in addressing potential challenges. To further enhance our preparedness, we conduct tabletop exercises that simulate various disaster scenarios. These exercises help train our teams to respond effectively and efficiently to potential events that could trigger a disaster recovery situation.

Progyny provides a robust information security management system that prioritizes the security and privacy of our members' sensitive information.