

## Agent Registration Agreement

This Agent Registration Agreement (“Registration Agreement”) is effective as of the date you (“you” or “Subscriber” or “Registering Agent”) entered into the Subscriber Agreement with Park Avenue Capital, LLC, d/b/a “MaxMD” (“MaxMD”) for the Service described therein (the “Agreement”), and this Registration Agreement is made a part of, and incorporated into, the Agreement.

### Recitals:

**WHEREAS**, as a subscriber to the Service, Subscriber will be required to conduct identity proofing and verification of individuals and entities applying for a Direct Certificate or Direct mdEmail under Subscriber’s account and subscription to the Service (“Authorized Users”);

**WHEREAS**, subject to the terms and conditions hereof, MaxMD, in its role as a Registration Authority, is willing to appoint Subscriber as a Registering Agent with the authority to vet and identify proof potential Authorized Users (“Vetted Authorized User”); and

**WHEREAS**, Subscriber (or “Registering Agent”) accepts such appointment as a Registering Agent pursuant to the terms and conditions hereof, acting through its customers and agents who have been trained on the Service and who have been designated to perform the duties of a Trusted Agent on behalf of Subscriber hereunder (“Trusted Agents”);

**NOW THEREFORE**, in consideration of the recitals, the mutual covenants and agreements made herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

### AGREEMENT:

**1. Defined Terms.** Capitalized terms used and not otherwise defined herein shall have the respective meanings set forth in MaxMD’s Certificate Practices Statement (“CPS”) located at <https://www.directmdemail.com/documents/DirectPolicy> and the Registration Practices Statement (“RPS”) located at <https://www.directmdemail.com/documents/DirectPolicy>.

**2. CPS and RPS Requirements.** The CPS and RPS outline the legal, commercial and technical principles and practices that MaxMD, as Registration Authority, employs and requires Registering Agents and Trusted Agents to employ in providing certification services. This document is a statement of the practices that MaxMD uses in approving, issuing, using and otherwise managing X.509 Digital Certificates and maintaining a Certificate-based public key infrastructure (“PKI”) applicable to the Certificates MaxMD uses. The CPS also defines the underlying certification processes for Vetted Authorized Users of Certificates and describes MaxMD’s Certification Authority (“CA”) and certificate repository operations, practices and requirements. The MaxMD CPS is a public statement of the practices of MaxMD and serves to notify all parties involved in the MaxMD PKI of their roles and responsibilities. It is imperative that Registering Agent and all Trusted Agents and Vetted Authorized Users and/or subscribers understand their responsibilities as outlined in the CPS and RPS. MaxMD has designated Registering Agent as a Registering Agent with the authority to designate [trained team members] as Trusted Agents to perform the gathering of documentation and vetting in accordance with this Registration Agreement and the CPS and RPS. MaxMD may update the CPS and RPS from time to time. MaxMD will post any changes to the CPS or RPS on the MaxMD website.

**3. Certain Registration Requirements.** The MaxMD Direct Health Information Service Provider (“HISP”) will not provide Certificates to a person or entity that is on a governmental denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business. Organizational Certificate applicants are required to include name, address, domain name, and evidence of the organization’s existence in the Certificate application. The requesting organization must be a HIPAA covered entity, a HIPAA business associate, or a healthcare-related organization that treats protected health information (“PHI”) with privacy and security protections that are equivalent to those required by HIPAA. Each organizational Certificate must represent a legally distinct entity. Registering Agent may rely on representation from the organization to verify the organization’s status as a valid legal entity in good standing for purposes of qualifying for a Direct Certificate.

#### **4. Registering Agent Responsibilities.**

(i) General. As Registering Agent, Subscriber agrees to comply with its responsibilities and obligations under the CPS and RPS and shall require Trusted Agents to do the same. Without limiting the foregoing, Registering Agent shall require each Trusted Agent to verify the included applicant's name and address using a reliable third-party database, a government database, or through Trusted Agent's communication with the entity or jurisdiction responsible for the organization's creation or recognition. If the Trusted Agent cannot use these sources to verify the name and address, then the Trusted Agent may verify the name and address using official company documentation that is submitted by the applicant, such as a business license, filed or certified articles of incorporation/organization, tax certificate, corporate charter, official letter, sales license, or other acceptable documents outlined in the RPS.

(ii) Inability to Verify Authorized User. If a Trusted Agent is unable to verify a Vetted Authorized User or a potential subscriber's name, address, date of birth, or government issued photo ID number, the Trusted Agent shall refuse to verify or authenticate the identity of the entity or individual. The name of each Vetted Authorized User (or Direct message recipient/sender) must be delivered to Registering Agent before the Vetted Authorized User will be provided with access to MaxMD's Direct Secure Messaging Service.

(iii) Maintenance of Records. Registering Agent shall, and shall require Trusted Agents to, maintain records of the identity verification process, including (i) Vetted Authorized Users' (Recipient/Senders') name, address, date of birth, government issued photo ID type and number, (ii) name and contact information of Trusted Agents performing identity proofing and/or certification, (iii) date and time verifications performed, and (iv) source used to perform verification (e.g., DMV, e-Verify, credit bureau).

(iv) Organizational Affiliation and LOA 3 or IAL 2 Direct Certificates. If a Certificate asserts an organizational affiliation between an individual and an organization, then the Trusted Agent will obtain documentation from the organization that recognizes the affiliation and obligates the organization to provide updates if the affiliation changes. For LOA 3 or IAL 2 Direct Certificate, information is verified using either an in-person or remote vetting process. These respective processes are documented in section 3 of the current DirectTrust CP which can be found at <https://www.directmdemail.com/documents/DirectPolicy>.

(v) Indemnity. Registering Agent shall indemnify, defend and hold harmless MaxMD, and its parent companies, subsidiaries, and their directors, officers, members, employees, agents and contractors for any breach by Registering Agent or any Trusted Agent of this Registration Agreement and will require Vetted Authorized Users (Senders/Recipients) to comply with their responsibilities as set forth in the CPS and RPS, including Section 9.9.

**5. Audits.** MaxMD, in its role as Registration Authority, may, at any time and from time to time, audit any or all Vetted Authorized User identity verification records, and Registering Agent shall ensure that Trusted Agents shall provide access to Registering Agent and Registration Authority to such records. The Trusted Agent should securely send this information to the Registration Authority and Registering Agent.

**6. Automatic Termination.** This Registration Agreement shall be coterminous with the Agreement and shall automatically terminate upon any termination of the Agreement.