

**DISTRICT OF COLUMBIA
OFFICE OF THE ATTORNEY GENERAL**

ASSURANCE OF VOLUNTARY COMPLIANCE

This Assurance of Voluntary Compliance¹ (“Assurance”) is entered into by the Attorneys General of Connecticut², the District of Columbia, and Oregon (referred to collectively as the “Attorneys General”) and Easy Healthcare Corporation (“Easy Healthcare”; collectively, with the Attorneys General, the “Parties”) to resolve the investigation by the Attorneys General into Easy Healthcare’s alleged violations of state unfair and deceptive practices acts (“Consumer Protection Acts”), as well as state laws requiring the safeguarding of personal information (“Personal Information Protection Acts”).

In consideration of their mutual agreement to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

I. INTRODUCTION

This Assurance constitutes a good faith settlement between Easy Healthcare and the Attorneys General of claims related to Easy Healthcare’s alleged sharing of Personal Information with third parties through its fertility-based Premom Ovulation Tracker mobile application (“Premom app”) without fully disclosing or obtaining Consumer consent for such information sharing. Easy Healthcare denies the allegations and denies any wrongdoing, and enters into this

¹ This Assurance of Voluntary Compliance shall, for all necessary purposes, also be considered an Assurance of Discontinuance.

² For ease of reference, this group will be referred to herein as the “Attorneys General” or individually as “Attorney General.” Such designations, however, as they pertain to Connecticut, shall refer to the Attorney General, both acting on his own behalf and as authorized by the Commissioner of the Department of Consumer Protection. “Connecticut Attorney General” shall mean only the Attorney General.

Assurance for settlement purposes only and solely to avoid the time and expense associated with litigation. Nothing in this Assurance shall be construed as an admission of liability or wrongdoing.

II. DEFINITIONS

1. For the purposes of this Assurance, the following definitions shall apply:
 - a. “Affirmative Express Consent” shall mean any freely given, specific, informed, and unambiguous indication of an individual’s wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual, apart from any “privacy policy,” “terms of service,” “terms of use,” or other similar document, of all information material to the provision of consent. Acceptance of a general or broad terms of use or similar document that contains descriptions of agreement by the individual along with other, unrelated information, does not constitute Affirmative Express Consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute Affirmative Express Consent. Likewise, agreement obtained through use of a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, does not constitute Affirmative Express Consent.

- b. “Clear and Conspicuous” shall mean that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
- i. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made in only one means.
 - ii. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 - iii. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 - iv. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

- v. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.
 - vi. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 - vii. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 - viii. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- c. “Consumer” shall mean a user or consumer in Connecticut, the District of Columbia, or Oregon who downloaded and used, or downloads and uses, the Premom app.
 - d. “Consumer Protection Acts” shall mean the citations listed in Appendix A.
 - e. “De-identified Information” means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable Consumer or a device linked to such Consumer, provided that Easy Healthcare: (1) takes reasonable measures to ensure that such information cannot be associated with such Consumer, including by third-party recipients of the information; and (2) publicly commits to process the

information only in de-identified form and not attempt to re-identify the information.

- f. “Easy Healthcare” shall mean Easy Healthcare Corporation, an Illinois corporation, and its affiliates, subsidiaries, successors and assigns, and its officers and senior employees with managerial responsibilities.
- g. “Effective Date” shall be August 1, 2023, or the date on which the FTC Proposed Order is signed and entered by the presiding district court judge, whichever is earlier.
- h. “FTC Proposed Order” means the proposed Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief in the matter of United States of America v. Easy Healthcare Corporation, d/b/a Easy Healthcare, signed by Easy Healthcare on March 27, 2023 and to be filed by the United States of America acting upon notification and authorization to the Attorney General of the United States by the Federal Trade Commission in the United States District Court for the Northern District of Illinois.
- i. “Health Information” shall mean individually identifiable medical records and other individually identifiable information relating to the past, present, or future physical or mental health or conditions of a Consumer, the provision of health care to a Consumer, or the past, present, or future payment for the provision of health care to a Consumer. It includes, but is not limited to, information about a Consumer concerning fertility, menstruation, sexual activity, pregnancy, and childbirth. It also includes any

individually identifiable information relating to health that is derived or extrapolated from non-health information (e.g., proxy, derivative, inferred, emergent, or algorithmic data).

- j. “Location Information” shall mean any data derived from technology that reveals a mobile device’s or Consumer’s precise location, including but not limited to Global Positioning System (GPS) coordinates, fine or coarse location data, cell tower information, or location information inferred from basic service set identifiers (BSSIDs), WiFi Service Set Identifiers (SSID) information, or Bluetooth receiver information. Data that reveals only a mobile device or Consumer’s general location (i.e., location within a radius of more than 1,750 feet) is not Location Information.
- k. “Necessary Purpose” shall mean a purpose relevant and reasonably necessary to the core functionality of Easy Healthcare’s mobile application and online services as represented by Easy Healthcare to the user. For purposes of this definition, Targeted Advertising shall be not considered a Necessary Purpose.
- l. “Personal Information” shall mean any individually identifiable information about an individual Consumer, including: (1) a first and last name; (2) a home or physical address, including street name and name of city or town; (3) Location Information; (4) online contact information, meaning an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to an

instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat identifier; (5) a screen or user name where it functions in the same manner as online contact information; (6) a telephone number; (7) a government-issued identification number, such as a driver's license, military identification, passport, Social Security number, or other personal identification number; (8) a credit card or other financial account information; (9) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, a processor serial number, an advertising ID, a hardware ID, an international mobile equipment identity, a Wi-Fi media access control ("MAC") address, a Bluetooth name, a Bluetooth MAC address, a router service set identifier, or a router MAC address; or (10) any information combined with any of (1) through (9) above. "Personal Information Protection Acts" shall mean the State citations listed in Appendix B.

- m. "Service Provider" shall mean any entity that: (i) receives, stores, or uses Personal Information collected by or on behalf of Easy Healthcare for and at the direction of Easy Healthcare and no other individual or entity; (ii) does not disclose the Personal Information, or any data derived therefrom, to any individual or entity other than Easy Healthcare or a subcontractor to such service provider bound to data processing terms no less restrictive than terms to which the service provider is bound, and (iii) does not use such information for any other purpose.

- n. “Software Development Kit” or “SDK” shall mean a set of software development tools, libraries, and sample code that can be used for some service or functionality for mobile applications or online services, such as to provide advertisements or push notifications. SDKs may be Service Providers or Third Parties based on their relationship with Easy Healthcare.
- o. “Third-Party” shall mean any entity, other than (1) Easy Healthcare; (2) a Service Provider of Easy Healthcare, or (3) any entity that uses Personal Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Easy Healthcare’s terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.
- p. “Targeted Advertising” means displaying advertisements to a Consumer where the advertisement is selected based on Personal Information obtained or inferred from a Consumer’s activities over time or across one or more nonaffiliated websites or online applications to predict such Consumer’s preferences or interests. For purposes of this definition, Targeted Advertising shall not include: (1) first party advertising (e.g., displaying advertisements to, or communications with, a Consumer based on that Consumer’s activities within Easy Healthcare’s own websites or mobile applications); (2) advertisements based on the context of a Consumer’s current search query, visit to an Internet website or online application; (3) advertisements directed to a Consumer in response to the Consumer’s request for information or feedback; or (4) processing of Personal

Information solely to measure or report advertising frequency, performance or reach.

III. APPLICATION

2. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to Easy Healthcare, its affiliates, subsidiaries, successors and assigns, and its officers and employees.

IV. INJUNCTIVE PROVISIONS

A. GENERAL COMPLIANCE

3. Easy Healthcare shall comply with the Consumer Protection Acts and Personal Information Protection Acts in connection with its collection, maintenance, and safeguarding of Personal Information.

4. Easy Healthcare shall not make any misrepresentations concerning the extent to which it maintains and protects the confidentiality, integrity, or security of Personal Information, including but not limited to:

- a. Its collection, use, storage or disclosure of Personal Information;
- b. The extent to which Consumers can control the privacy of Personal Information;
- c. The extent to which Easy Healthcare makes or has made Personal Information accessible to any Service Providers or Third-Parties, and the purposes for which Service Providers or Third-Parties are permitted access to such Personal Information;

- d. The steps Easy Healthcare takes or has taken to verify the privacy or security protections of any Service Provider or Third-Party who is provided access to Personal Information; and
 - e. The extent to which Easy Healthcare protects the privacy, confidentiality, integrity, and security of Personal Information.
5. Easy Healthcare shall not make any misrepresentations concerning the efficacy of its products or services.

B. PRIVACY PROGRAM

6. Within sixty (60) days of the Effective Date, Easy Healthcare shall implement and maintain a comprehensive information privacy program governing the collection, storage, use, and disclosure of Personal Information (“Privacy Program”). The Privacy Program shall, at a minimum, include the specific privacy safeguards set forth in Paragraphs 10 through 23 of this Assurance.

7. Within sixty (60) days of the Effective Date, Easy Healthcare shall designate one or more individuals with appropriate background or experience who shall be responsible for implementing and maintaining the Privacy Program. Easy Healthcare shall notify the Attorneys General of the title(s) of the individual(s) designated pursuant to this Paragraph within thirty (30) days of the above deadline.

8. Easy Healthcare shall ensure that the role of the designated individual(s) referenced in Paragraph 7 includes advising the Chief Executive Officer and Chief Financial Officer on at least a semi-annual basis of the privacy risks faced by Easy Healthcare and the privacy implications of Easy Healthcare’s decisions impacting Consumers.

9. Easy Healthcare may satisfy the implementation and maintenance of the Privacy Program and the safeguards required by this Assurance through review and, if necessary, updating of an existing privacy program or safeguards, provided that such program or safeguards meet the requirements set forth in this Assurance.

C. PRIVACY PROGRAM: SPECIFIC SAFEGUARDS

10. **Data Minimization:** Easy Healthcare shall not collect Personal Information except for a specified, legitimate Necessary Purpose(s).

11. **Purpose Limitations:** Easy Healthcare shall not store, use, disclose, or permit collection of Personal Information in any manner incompatible with the specified Necessary Purpose(s) for which such information was collected. Nothing in this Paragraph shall preclude Easy Healthcare from using Personal Information for a permissible secondary purpose. For purposes of this Paragraph, “permissible secondary purpose” shall mean: (i) internal research to develop, improve or repair a product or service for which such Personal Information was collected; or (ii) Targeted Advertising consistent with the provisions of this Assurance, provided that Easy Healthcare provides Consumers the ability to opt out of such advertising.

12. **Personal Information Inventory:** Easy Healthcare shall conduct annual inventories of the Premom app to document the extent to which such application collects, stores, uses, discloses, or permits collection of Personal Information.

13. **Privacy Policy:** Easy Healthcare shall provide Consumers with a privacy policy that Clearly and Conspicuously discloses:

- a. the categories of Personal Information that Easy Healthcare collects;

- b. the type, source, and precision of the Location Information that will be collected as well as the frequency of the collection;
- c. the Necessary Purpose(s) for which Personal Information is collected, how such information will be used;
- d. any permissible secondary purpose(s) for which Easy Healthcare will use Personal Information, including whether such information is used for Targeted Advertising, and if so, the means by which Consumers may opt out of such advertising;
- e. how long Personal Information will be retained;
- f. the specific Third-Parties with whom Easy Healthcare shares Personal Information, whether actively or passively, the categories of Personal Information shared, and the purpose(s) for such sharing;
- g. the steps Easy Healthcare takes or has taken to verify the privacy and data security protections of such Service Providers and Third-Parties; and
- h. whether Consumers have control over their Personal Information, and if so, what kind of control they have and how to exercise that control.

14. **Notice of Material Changes:** Easy Healthcare shall not collect, store, use, disclose, or permit collection of Personal Information in any manner that is materially inconsistent with its privacy policy. Easy Healthcare shall provide Clear and Conspicuous notice to Consumers of any material change(s) to its privacy policy impacting the manner in which it collects, stores, uses, discloses, or permits collection of Consumers' Personal Information prior to any such changes(s) taking effect.

15. **Prohibition Against Disclosure of Health Information without Affirmative Express Consent:** Easy Healthcare shall not disclose Health Information to Third-Parties without first obtaining Affirmative Express Consent. When obtaining Affirmative Express Consent required under this Paragraph, Easy Healthcare must provide notice that Clearly and Conspicuously states the categories of Health Information that will be disclosed to Third-Parties, the identities of such Third Parties, the purposes for Easy Healthcare's disclosures of such Health Information, and what the Third-Parties are permitted to do with the Health Information. Under no circumstances may Easy Healthcare disclose Health Information to Third Parties for Targeted Advertising.

16. **Prohibition Against Disclosure of Location Information without Affirmative Express Consent:** Easy Healthcare shall not disclose Location Information to Third Parties without first obtaining Affirmative Express Consent. When obtaining Affirmative Express Consent required under this Paragraph, Easy Healthcare must provide notice that Clearly and Conspicuously states the type, source, and precision of the Location Information that will be disclosed to Third Parties, the identities of such Third Parties, the purposes for Easy Healthcare's disclosures of such Location Information, and what the Third Parties are permitted to do with the Location Information.

17. **Revocation of Consent:** Easy Healthcare shall allow Consumers to revoke any previously granted Affirmative Express Consent for the disclosing of the Consumer's Health Information or Location Information to Third Parties. Following a Consumer's revocation of Affirmative Express Consent, Easy Healthcare shall cease disclosing, the Consumer's Health

Information or Location Information to Third Parties for the purpose(s) covered by the revocation on a going-forward basis.

18. **Right to Delete:** Easy Healthcare shall provide an easily accessible method by which a Consumer may request deletion of the Consumer's Personal Information. Easy Healthcare shall timely (within forty-five (45) days after receipt of the request, where such time period may be extended by Easy Healthcare by forty-five (45) days when reasonably necessary, provided Easy Health informs the Consumer of any such extension within the initial forty-five (45) day response period and the reason for the extension) process all such requests and provide confirmation of the deletion to the Consumer.

- a. Easy Healthcare may comply with a Consumer's request to delete their Personal Information by: (i) permanently and completely erasing the Personal Information on its existing systems with the exception of archived or back-up systems; or (ii) maintaining only De-Identified Information for that Consumer.
- b. Easy Healthcare may delay compliance with the Consumer's request to delete, with respect to data stored on an archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used.
- c. Easy Healthcare shall not be required to comply with a Consumer's request to delete the Consumer's Personal Information if the Personal Information is necessary for Easy Healthcare to (i) complete the transaction for which the Personal Information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or

service requested by the consumer, or reasonably anticipated within the context of Easy Healthcare's ongoing business relationship with the Consumer, or otherwise perform a contract between the Easy Healthcare and the Consumer; (ii) detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity; (iii) debug to identify and repair errors that impair existing intended functionality; (iv) exercise free speech, ensure the right of another Consumer to exercise his or her right of free speech, or exercise another right provided for by law; (v) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when deletion of the Personal Information is likely to render impossible or seriously impair the achievement of such research, if the Consumer has provided informed consent; (vi) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the Consumer's relationship with the Easy Healthcare; (vii) comply with a legal obligation; or (viii) otherwise use the Consumer's Personal Information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

- d. In the event that a Consumer's Personal Information cannot be deleted due to a listed exception in subsection (c) of this Paragraph, Easy Healthcare shall timely provide the basis to not delete the Personal Information to the Consumer.

- e. Upon receipt of an actionable deletion request, Easy Healthcare shall also notify any Service Providers and Third Parties that collected or received such Personal Information of the Consumer's request.

Easy Healthcare's obligations under this Paragraph shall not restrict Easy Healthcare's ability to comply with federal, state, or local laws or regulations, or to comply with any civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local or other governmental authorities.

19. **Employee Training:** Easy Healthcare shall provide employee training concerning its Privacy Program on an ongoing and regular basis. In particular, such training shall include privacy issues related to reproduction and reproductive rights, as well as the risks that women face or could face, as a result of privacy lapses while using Easy Healthcare's Premom app or online services. Training shall be conducted no less than once in a calendar year.

D. PRIVACY PROGRAM: SERVICE PROVIDERS AND THIRD-PARTIES

20. **Due Diligence:** Prior to disclosing or permitting collection of Personal Information, Easy Healthcare shall implement, maintain, and document a process for selecting Service Providers and Third-Parties capable of safeguarding Personal Information. As part of this process, Easy Healthcare shall:

- a. document its review of Service Providers and Third-Parties' privacy policies and practices; verify that the privacy policies of Service Providers and Third-Parties are consistent with Easy Healthcare's obligations under this Assurance; and

- b. only select Service Providers and Third-Parties with privacy policies that are available on their website homepages or which are otherwise easily accessible by Consumers.

Easy Healthcare shall retain documentation reflecting its efforts to review Service Providers' and Third-Parties' privacy policies and privacy and data security procedures.

21. **Written Contracts:** Prior to disclosing Personal Information to a Service Provider or otherwise permitting the Service Provider to collect Personal Information, Easy Healthcare shall enter into written contracts or agreements³ requiring the Service Provider to:

- a. refrain from retaining, using, or disclosing the Personal Information received from Easy Healthcare for any purposes other than those specified in the contract or agreement;
- b. appropriately safeguard the confidentiality, integrity, and security of Personal Information; and
- c. securely destroy/dispose of Personal Information after its relationship with Easy Healthcare is terminated.⁴

Easy Healthcare shall retain copies of such written agreements or contracts applicable to such Service Providers and any other documentation demonstrating a Service Provider's commitment to comply with the foregoing practices.

22. **Monitoring:** Easy Healthcare shall implement and maintain policies and procedures that are reasonably designed to ensure that there are processes in place to monitor

³ For purposes of Paragraphs 21 and 22, "agreement" may include standard terms.

⁴ In the case where a Service Provider will not agree to such language in the agreement, Easy Healthcare will, upon termination of the agreement, instruct the Service Provider, in writing, to security destroy/dispose of Personal Information.

Service Providers and Third-Parties to identify material inconsistencies between their collection of Personal Information from the Premom app and the terms of any written contract or agreement such Service Provider or Third Party may have with Easy Healthcare. Easy Healthcare shall retain documentation of such efforts. Such monitoring shall include audits, assessments, reviews or testing of Service Providers' and Third Parties' collection of Personal Information through SDKs used in connection with the Premom app.

23. **Materially Inconsistent Collection Practices:** Easy Healthcare shall take appropriate action against any Service Provider or Third-Party that Easy Healthcare has reason to know is collecting Personal Information in a manner materially inconsistent with the privacy policy applicable to the Premom app, and/ or the terms of any written agreement or contract it may have with Easy Healthcare with regards to the Premom app, up to and including termination of its relationship with that Third-Party or Service Provider.

E. PRIVACY RISK ASSESSMENTS

24. Easy Healthcare shall conduct a privacy risk assessment that assesses and documents the potential risks that its collection, use, storage, or sharing of Personal Information has on Consumers' privacy ("Privacy Risk Assessment").

25. The Privacy Risk Assessment shall also: (i) consider the risks that women face, or could face, as a result of privacy or security lapses while using Easy Healthcare's Premom mobile application or online services; (ii) consider the impact of any such risks; and (iii) document Easy Healthcare's efforts to mitigate any such risks.

26. The assessment period for the Privacy Risk Assessment shall cover the first one hundred and eighty (180) days after the the Privacy Program required by Section IV has been put in place.

27. Easy Healthcare shall provide a copy of the Privacy Risk Assessment to the Attorneys General within sixty (60) days of completion of the report.

28. In the event that Easy Healthcare obtains an initial privacy and information security assessment pursuant to Section VIII of the FTC Proposed Order, such assessment may be submitted in satisfaction of the Privacy Risk Assessment so long as it satisfies the requirements of Paragraphs 24 and 25.

29. Easy Healthcare shall make any subsequent privacy and information security assessments performed pursuant to Section VIII of the FTC Proposed Order available to the Attorneys General upon request.

F. INFORMATION SECURITY PROGRAM

30. Within sixty (60) days after the Effective Date, Easy Healthcare shall implement and maintain a comprehensive information security program designed to protect the confidentiality, integrity, and security of Consumers' Personal Information ("Information Security Program"). The Information Security Program shall, at a minimum, include the specific information security safeguards set forth in Paragraphs 35 and 36 of this Assurance.

31. Easy Healthcare's Information Security Program shall be documented and shall contain administrative, technical, and physical safeguards appropriate to: the size and complexity of Easy Healthcare's operations; the nature and scope of Easy Healthcare's operations; and the sensitivity of Consumers' Personal Information.

32. Within sixty (60) days of the Effective Date, Easy Healthcare shall designate one or more individuals with appropriate background or experience who shall be responsible for implementing and maintaining the Information Security Program. Easy Healthcare shall notify the Attorneys General of the title(s) of the individual(s) designated pursuant to this Paragraph within thirty (30) days of the above deadline.

33. Easy Healthcare shall ensure that the role of the designated individual(s) referenced in Paragraph 32 includes advising the Chief Executive Officer and Chief Financial Officer on at least a semi-annual basis of Easy Healthcare's security posture, the security risks faced by Easy Healthcare, and security implications of Easy Healthcare's decisions impacting Consumers.

34. Easy Healthcare may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Assurance through review and, if necessary, updating of an existing information security program or existing safeguards, provided that such existing safeguards meet the requirements set forth in this Assurance.

G. SPECIFIC INFORMATION SECURITY SAFEGUARDS

35. **Data Security Risk Assessments:** Easy Healthcare shall perform regular risk assessments to identify and assess risks to the security of Consumers' Personal Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information. Easy Healthcare shall put in place measures that are designed to appropriately remediate such risks and maintain documentation of any remedial steps taken as a result of such assessments, including any remedial steps taken as a result of any penetration tests that Easy Healthcare may conduct.

36. **Data Retention:** Easy Healthcare shall maintain data retention policies and procedures that include, at a minimum, specific schedules for retention of Personal Information for only as long as reasonably necessary to fulfill the Necessary Purpose for which the Personal Information was collected.

H. INFORMATION SECURITY ASSESSMENT

37. Easy Healthcare shall obtain an information security assessment and report from a third-party assessor (“Third-Party Assessor”) regarding its compliance with its Information Security Program (“Information Security Assessment”).

38. The Third-Party Assessor shall prepare a report (“Information Security Report”) that shall:

- a. Set forth the specific administrative, technical, and physical safeguards maintained by Easy Healthcare to protect Personal Information; and
- b. Explain the extent to which such safeguards that have been implemented meet the requirements of Easy Healthcare’s Information Security Program, taking into account Easy Healthcare’s size and complexity, the nature and scope of Easy Healthcare’s activities, and the sensitivity of the Personal Information maintained by Easy Healthcare.

39. The assessment period for the Information Security Report shall cover the first one hundred and eighty (180) days after the Information Security Program required by Section IV.F has been put in place.

40. Easy Healthcare shall provide a copy of the Information Security Report to the Attorneys General within sixty (60) days of completion and delivery of the Information Security Report to Easy Healthcare.

41. In the event that Easy Healthcare obtains an initial privacy and information security assessment pursuant to Section VIII of the FTC Proposed Order, Easy Healthcare may satisfy compliance with the Information Security Report requirements of Paragraphs 37–39 above by providing a copy of such initial assessment to the Attorneys General within five (5) days of submitting the assessment to the Federal Trade Commission.

42. Easy Healthcare shall make any subsequent privacy and information security assessments performed pursuant to Section VIII of the FTC Proposed Order available to the Attorneys General upon request.

VII. PAYMENT TO THE STATES

43. Easy Healthcare shall pay One Hundred Thousand Dollars (\$100,000.00) to the Attorneys General. Said payment is premised upon the truthfulness, accuracy, and completeness of Easy Healthcare's financial statements submitted to the Attorneys General. Said payment shall be divided and paid by Easy Healthcare directly to each of the Attorneys General in an amount designated by the Attorneys General, and communicated to Easy Healthcare along with payment instructions. Payment shall be made no later than thirty (30) days after the Effective Date of this Assurance, except that where state law requires judicial or other approval of the Assurance, payment shall be made no later than thirty (30) days after notice from the relevant Attorney General that such final approval for the Assurance has been secured.

44. Of the total amount, Easy Healthcare will pay Thirty-Three Thousand Three Hundred Thirty-Three Dollars and Thirty-Three Cents (\$33,333.33) to the Attorney General for the District of Columbia. Said payment shall be used by the Attorney General for the District of Columbia for such purposes that may include, but are not limited to, being placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid/ restitution fund or revolving fund, used to defray costs of the inquiry leading hereto, or for attorneys' fees and other costs of investigation, or for other uses permitted by state law, at the sole discretion of the Attorney General for the District of Columbia.

VII. PRESERVATION OF AUTHORITY

45. Nothing in this Assurance shall be construed to limit the authority or ability of an Attorney General to protect the interests of his/her State or the people of his/her State. This Assurance shall not bar the Attorney General or any other governmental entity from enforcing laws, regulations, or rules against Easy Healthcare for conduct subsequent to or otherwise not covered by this Assurance. Further, nothing in this Assurance shall be construed to limit the ability of the Attorney General to enforce the obligations that Easy Healthcare has under this Assurance.

VIII. GENERAL PROVISIONS

46. The Parties understand and agree that this Assurance shall not be construed as an approval or a sanction by the Attorneys General of Easy Healthcare's business practices, nor shall Easy Healthcare represent that this Assurance constitutes an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Attorneys General to take any action in response to any information submitted pursuant to this Assurance shall not be

construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor shall it preclude action thereon at a later date.

47. Nothing contained in this Assurance is intended to be, and shall not in any event be construed or deemed to be, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Easy Healthcare or of any fact or violation of any law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind.

48. Nothing in this Assurance shall be construed as relieving Easy Healthcare of the obligation to comply with all applicable state and federal laws, regulations, and rules, nor shall any of the provisions of this Assurance be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

49. As to each individual signatory State, this Assurance shall be governed by the laws of that State without regard to any conflict of laws principles.

50. Easy Healthcare shall deliver a copy of this Assurance to, or otherwise fully apprise, each of its current officers of the rank of executive vice president or above, the executive management officer having decision-making authority with respect to the subject matter of this Assurance, and each member of its Board of Directors within ninety (90) days of the Effective Date. Easy Healthcare shall deliver a copy of this Assurance to, or otherwise fully apprise, any new officers of the rank of executive vice president or above, new executive management officer having decision-making authority with respect to the subject matter of this Assurance, and each new member of its Board of Directors, within ninety (90) days from which such person assumes his/her position with Easy Healthcare.

51. In states where statute requires that this Assurance be filed with and/or approved by a court, Easy Healthcare consents to the filing of this Assurance and to its approval by a court, and authorizes the Attorneys General in such states to represent that Easy Healthcare does not object to the request that the court approve the Assurance. Easy Healthcare further consents to be subject to the jurisdiction of such courts (if legally required) for the exclusive purposes of having such courts approve or enforce this Assurance. To the extent that there are any court costs associated with the filing of this Assurance (if legally required), Easy Healthcare agrees to pay such costs.

52. Easy Healthcare shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Assurance or for any other purpose that would otherwise circumvent any term of this Assurance. Easy Healthcare shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Assurance.

53. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Assurance may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

54. The undersigned Easy Healthcare representatives state that they are authorized to enter into and execute this Assurance of Voluntary Compliance on behalf of Easy Healthcare and, further agree to execute and deliver all authorizations, documents and instruments which are necessary to carry out the terms and conditions of this Assurance of Voluntary Compliance.

55. Easy Healthcare agrees that this Assurance does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and Easy Healthcare further waives any right to attorneys' fees related to this Assurance that may arise under such statute, regulation, or rule.

56. This Assurance shall not be construed to waive any claims of sovereign immunity the States may have in any action or proceeding.

IX. SEVERABILITY

57. If any clause, provision, or section of this Assurance shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Assurance and this Assurance shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

X. NOTICE/DELIVERY OF DOCUMENTS

58. Whenever Easy Healthcare shall provide notice to the Attorney General for the District of Columbia under this Assurance, that requirement shall be satisfied by sending notice to:

Jennifer Rimm
Office of Consumer Protection
Office of the Attorney General for the District of Columbia
400 6th Street NW, Washington, DC 20001

59. Any notices or other documents sent to Easy Healthcare pursuant to this Assurance shall be sent to the following address:

Attn: Sherry Liu
Easy Healthcare Corporation
360 Shore Dr. Unit B
Burr Ridge, IL 60527

60. All notices or other documents to be provided under this Assurance shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall have been deemed to be sent upon mailing. Any party may update its address by sending written notice to the other party.

Consented and agreed to by:

Easy Healthcare Corporation

By: XIAOLIAN LIU Date: 03/27/2023
Xiaolin Liu
Chief Executive Officer

**DISTRICT OF COLUMBIA
OFFICE OF ATTORNEY GENERAL**

**BRIAN L. SCHWALB
ATTORNEY GENERAL**

By:  _____

Date: 3/29/2023

JENNIFER RIMM

Deputy Director

Office of Consumer Protection

Public Advocacy Division

Office of the Attorney General for the District of Columbia

400 Sixth Street, N.W.

Washington, D.C. 20001

Tel: 202-724-5191

Fax: 202-741-5956

Email: jennifer.rimm@dc.gov

Appendix A

STATE	CONSUMER PROTECTION ACTS
Connecticut	Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b <i>et seq.</i>
District of Columbia	Consumer Protection Procedures Act, D.C. Code §§ 28-3901 <i>et seq.</i>
Oregon	Oregon Unlawful Trade Practices Act, ORS 646.605 <i>et seq.</i>

Appendix B

STATE	PERSONAL INFORMATION PROTECTION ACTS
Connecticut	Safeguarding of Personal Information, Conn. Gen. Stat. § 42-471
District of Columbia	District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851 <i>et seq.</i>
Oregon	Oregon Consumer Information Protection Act, ORS 646A.600 <i>et seq.</i>