UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

UNITED STATES OF AMERICA, Plaintiff, v. EASY HEALTHCARE CORPORATION., a corporation, d/b/a EASY HEALTHCARE, Defendant.	**Case No. 1:23-cv-3107**

STIPULATED ORDER FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("Commission"), filed its Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Relief ("Complaint"), for a permanent injunction, civil penalties, and other relief in this matter, pursuant to Sections 13(b), 19, and 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b), 57b, and 56(a)(1). Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Permanent Injunction, Civil Penalty Judgment, and Other Relief ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.

2. The Complaint charges that Defendant participated in deceptive and unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and in violation of the Health

Breach Notification Rule, 16 C.F.R. § 318.

3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.

4. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agree to bear their own costs and attorney fees.

5. Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

A. "**Affected Work Product**" means any models or algorithms developed in whole or in part using Covered Information collected from Covered Users.

B. "**Affirmative Express Consent**" means 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.

C. "**App Event**" means any data disclosed to, or collected by, a third party via its Software Development Kit, application programing interface, pixel, or other method for tracking users' interactions with Defendant's services or products.

D. "**Breach of Security**" means, with respect to Unsecured PHR Identifiable Health Information of an individual in a Personal Health Record, any acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.

E. "**Clear and Conspicuous**" or "**Clearly and Conspicuously**" means 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:

1. 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.

2. 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.

3. 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.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. 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.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. 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.

F. "**Covered Business**" means Defendant, any business that Defendant controls, directly or indirectly.

G. "**Covered Incident**" means any instance of a violation of Section I, II, or III of this Order.

H. "**Covered Information**" means information from or about an individual consumer including, but not limited to Personal Information, Health Information, or PHR Identifiable Health Information.

I. "**Covered User**" means any individual consumer who downloaded or used the Premom Ovulation Tracker mobile application.

J. "**Defendant**" means Easy Healthcare Corporation, a corporation, also doing business as Easy Healthcare, and its successors and assigns.

K. "**Delete**," **"Deleted**," or "**Deletion**" means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

L. "**Health Care Provider**" means a provider of services (as defined in 42 U.S.C. § 1395x(u)), a provider of medical or other services (as defined in 42 U.S.C. § 1395x(s)), and any other person furnishing healthcare services or supplies.

M. "**Health Information**" means medical records and other individually identifiable information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. It includes, but is not limited to, information 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). Health Information includes PHR Identifiable Health Information, as defined below, and Health Information associated with Personal Information, as defined below.

N. "**Individually Identifiable Health Information**" means any information, including demographic information, collected from an individual that: (1) is created or received by a Health Care Provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision

of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and: (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

O. "**Location Information**" means any data 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, and any data combined with any such data. Data that reveals only a mobile device or consumer's general location (e.g., zip code or location with a precision of one kilometer or more) is not Location Information.

P. "**Personal Health Record**" means an electronic record of PHR Identifiable Health Information on an individual that can be drawn from multiple sources, and that is managed, shared, and controlled by or primarily for the individual.

Q. "**Personal Information**" means any individually identifiable information about an individual collected online, 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.

R. "**PHR Identifiable Health Information**" means Individually Identifiable Health Information, and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and (2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

S. "**Software Development Kit**" means the code necessary to integrate a Third Party's software—including advertisements—into an application, Web site, or other online service.

U. "**Third Party**" or "**Third Parties**" means any individual or entity other than: (1) Defendant; (2) a service provider of Defendant that: (i) uses or receives Covered Information collected by or on behalf of Defendant for and at the direction of the Defendant and no other individual or entity, (ii) does not disclose the data, or any individually identifiable information derived from such data, to any individual or entity other than Defendant 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 the data for any other purpose; or (3) any entity that uses Covered Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, (ii) to enforce Defendant's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

V. "**Unsecured**" means PHR Identifiable Health Information that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009, 42 U.S.C. § 17932(h)(2).

ORDER

I. BAN ON DISCLOSURE OF HEALTH INFORMATION FOR ADVERTISING PURPOSES

IT IS ORDERED that

A. Defendant; Defendant's officers, agents, employees, and attorneys; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, are permanently restrained and enjoined from disclosing Health Information to Third Parties for Advertising Purposes.

B. For purposes of this Section, Advertising Purposes means advertising, marketing promoting, offering, offering for sale, or selling any products or services on, by, or through Third Party websites, Third Party mobile applications, or Third Party services. Advertising Purposes shall not include: (i) reporting and analytics related to understanding advertising and advertising effectiveness, such as statistical reporting, traffic analysis, understanding the number of and type of ads served, or conversion measurement, provided that any Third Party reporting or analytics service is restricted from using any Covered Information received from or provided to Defendant for any purpose other than to provide the reporting and analytics services to Defendant; (ii) communications, services, or products requested by a consumer that are sent by Defendant directly to the consumer, such as Defendant texting, emailing, or mailing a consumer, or showing content on Defendant's own properties to a consumer; or (iii) contextual advertising, meaning non-personalized advertising shown as part of a consumer's current interaction with Defendant's

websites or mobile applications, provided that the consumer's Covered Information is not disclosed to a Third Party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with Defendant's websites or mobile applications.

II. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS FURTHER ORDERED that Defendant; Defendant's officers, agents, employees, and attorneys; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with advertising, marketing, promoting, offering, offering for sale, or selling any product or service are permanently restrained and enjoined from misrepresenting or assisting others, in any manner, expressly or by implication:

A. the extent to which they collect, maintain, use, disclose, or permit access to any Covered Information, or protect the privacy, confidentiality, security, or integrity of any Covered Information;

B. the extent to which the Covered Business collects, maintains, uses, discloses, deletes, or permits or denies access to any Covered Information, or the extent to the Covered Business protects the availability, confidentiality, or integrity of any Covered Information;

C. the purposes for which the Covered Business, or any entity to whom the Covered Business discloses or permits access to Covered Information, collects, maintains, uses, discloses, or permits access to any Covered Information;

D. the extent to which a consumer can maintain privacy and anonymity associated with the consumer's use of products or services offered by Covered Businesses;

E. the extent to which consumers may exercise control over the Covered Business' collection of, maintenance of, use of, deletion of, disclosure of, or permission of access to Covered Information, and the steps a consumer must take to implement such controls; and

F. the extent to which the Covered Business otherwise protects the privacy, security, availability, confidentiality, or integrity of Covered Information.

III. PROHIBITION AGAINST DISCLOSURE OF HEALTH INFORMATION WITHOUT AFFIRMATIVE EXPRESS CONSENT AND NOTICE

IT IS FURTHER ORDERED that

A. Defendant; Defendant's officers, agents, employees, and attorneys; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, in connection with any product or service, are permanently restrained and enjoined from disclosing Health Information to Third Parties for non-Advertising Purposes, without first obtaining Affirmative Express Consent.

B. For purposes of this Section, Advertising Purposes means advertising, marketing, promoting, offering, offering for sale, or selling any products or services on, by, or through Third Party websites, Third Party mobile applications, or Third Party services. Advertising Purposes shall not include: (i) reporting and analytics related to understanding advertising and advertising effectiveness, such as statistical reporting, traffic analysis, understanding the number of and type of ads served, or conversion measurement, provided that any Third Party reporting or analytics services is restricted from using any Covered Information received from or provided to Defendant for any purpose other than to provide the reporting and analytics services to Defendant; (ii) communications, services, or products requested by a consumer that are sent by Defendant directly to the consumer, such as Defendant texting, emailing, or mailing a consumer, or showing content on Defendant's own properties to a consumer; or (iii) contextual advertising,

meaning non-personalized advertising shown as part of a consumer's current interaction with Defendant's websites or mobile applications, provided that the consumer's Covered Information is not disclosed to a Third Party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with Defendant's websites or mobile applications.

C. When obtaining Affirmative Express Consent required under this Section, Defendant must provide notice Clearly and Conspicuously that states the categories of Health Information that will be disclosed to Third Parties, the identities of such Third Parties, all purposes for Defendant's disclosures of such Health Information, what the Third Party is permitted to do with the Health Information, and whether or not any of the Health Information is protected under federal or state laws, including HIPAA or the California Consumer Privacy Act.

IV. HEALTH BREACH NOTIFICATIONS

IT IS FURTHER ORDERED that

A. Defendant, for any Covered Business, following the discovery of a Breach of Security of Unsecured PHR Identifiable Health Information that is in a Personal Health Record maintained or offered by any Covered Business (including, but not limited to, the Premom Ovulation Tracker mobile application, shall:

1. notify each individual who is a citizen or resident of the United States whose Unsecured PHR Identifiable Health Information was acquired by an unauthorized person as a result of such Breach of Security;

2. notify the Federal Trade Commission; and

3. notify prominent media outlets in a state or jurisdiction, if the Unsecured PHR Identifiable Health Information of five hundred (500) or more residents of such state or

jurisdiction is, or is reasonably believed to have been, acquired during such Breach of Security.

B. For the purposes of this Section, a Breach of Security shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known to Defendant. Defendant shall be deemed to have knowledge of a Breach of Security if such breach is known, or reasonably should have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of Defendant.

C. Except as otherwise provided, all notifications to individuals or the media required under this Section shall be sent without unreasonable delay and in no case later than sixty (60) calendar days after the discovery. If a law enforcement official determines that a notification, notice, or posting required under this Section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed. This Subsection shall be implemented in the same manner as provided under 45 CFR 164.528(a)(2), in the case of a disclosure covered under such section.

D. Defendant providing notice under Subsection IV.A.1 shall do so by providing it in the following form:

1. Written notice, by first-class mail to the individual at the last known address of the individual, or by email or within-application messaging, if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice. If the individual is deceased, Defendant must provide such notice to the next of kin of the individual if the individual had provided contact information for his or her next of kin, along with authorization to contact them. The notice may be provided in one or more mailings as information is available.

2. If, after making reasonable efforts to contact all individuals to whom

notice is required under Subsection IV.A.1, through the means provided in Subsection IV.D.1, Defendant finds that contact information for ten (10) or more individuals is insufficient or out-of-date, Defendant shall provide substitute notice, which shall be reasonably calculated to reach the individuals affected by the Breach of Security, in the following form:

a. Through a conspicuous posting for a period of ninety (90) days on the home page of its Web site; or

b. In major print or broadcast media, including major media in geographic areas where the individuals affected by the Breach of Security likely reside. Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least ninety (90) days, where an individual can learn whether or not the individual's PHR Identifiable Health Information may be included in the Breach of Security.

3. In any case deemed by Defendant to require urgency because of possible imminent misuse of Unsecured PHR Identifiable Health Information, Defendant may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under Subsection IV.E.1.

E. Defendant shall, in accordance with Subsection IV.A.2, provide notice to the Federal Trade Commission following the discovery of a Breach of Security. If the Breach of Security involves the Unsecured PHR Identifiable Health Information of five hundred (500) or more individuals, then such notice shall be provided as soon as possible and in no case later than ten (10) business days following the date of discovery of the Breach of Security. If the Breach of Security involves the Unsecured PHR Identifiable Health Information of fewer than five hundred (500) individuals, Defendant may maintain a log of any such Breach of Security, and submit

such a log annually to the Federal Trade Commission no later than sixty (60) calendar days following the end of the calendar year, documenting Breaches of Security from the preceding calendar year. Unless otherwise directed by a Commission representative in writing, Defendant must submit all notices and logs required under this Subsection to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "U.S. v. Easy Healthcare Corporation."

F. Regardless of the method by which notice is provided to individuals, the Federal Trade Commission, or the media under this Section, notice of a Breach of Security shall be in plain language and include, to the extent possible, the following:

1. A brief description of what happened, including the date of the Breach of Security and the date of the discovery of the Breach of Security, if known;

2. A description of the types of PHR Identifiable Health Information that were involved in the Breach of Security (such as full name, Social Security number, date of birth, home address, account number, or disability code);

3. Steps individuals should take to protect themselves from potential harm resulting from the Breach of Security;

4. A brief description of what the entity that suffered the Breach of Security is doing to investigate the breach, to mitigate harm, and to protect against any further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a tollfree telephone number, an email address, Web site, or postal address.

V. NOTICE TO USERS

IT IS FURTHER ORDERED that, within twenty-eight (28) days of entry of this Order, Defendant shall post Clearly and Conspicuously on the home page of Defendant's websites (https://healthcare-manager.com; http://premom.com) and the home screen of Defendant's mobile application (Premom Ovulation Tracker), a link to an exact copy of the notice attached hereto as Exhibit A ("Notice"). Defendant must leave this Notice in place for six (6) months after posting it. Defendant must also email the Notice to Covered Users that downloaded and used Premom from November 2017 to August 2022, *provided however*, that if Defendant does not have email information for any such Covered User, Defendant must send the Notice to that Covered User through Defendant's primary means of communicating with that Covered User (such as a notification within Defendant's mobile application). Defendant shall not include with the Notice any other information, documents, or attachments.

VI. DELETION OF COVERED INFORMATION

IT IS FURTHER ORDERED that, within forty-five (45) days of entry of this Order:

A. Defendant must

1. identify all Third Parties that received Covered Information of Covered Users from Defendant in any form, including hashed or encrypted Covered Information, identify the Covered Information of Covered Users received, provide a copy of the Complaint and Order to all Third Parties that received Covered Information, and notify all such Third Parties in writing that the Federal Trade Commission alleged that Defendant disclosed Covered Information of Covered Users in a manner that was unfair or deceptive and in violation of the FTC Act; and

2. instruct Jiguang and Umeng to Delete all Covered Information received from Defendant of Covered Users that downloaded and used the Premom Ovulation Tracker mobile application from November 2017 through August 2020 and demand written confirmation that all Covered Information has been deleted; and (ii) AppsFlyer, Inc. and Google, LLC, to Delete all Health Information collected respectively through the AppsFlyer SDK or the Google Analytics for Firebase SDK of Covered Users that downloaded and used Premom from November 2017 through August 2022 and demand written confirmation that all the Health Information of such Covered Users has been deleted.

B. Defendant's instruction to each such Third Party under Subsection A shall include a description of the Covered Information or Health Information, as relevant, of Covered Users shared with the Third Party during the relevant time period. Defendant must provide all instructions sent to the Third Parties to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "United States v. Easy Healthcare Corporation."

C. Defendant shall not disclose any Covered Information in any form, including hashed or encrypted Covered Information, to any Third Party identified in Subsection A above until Defendant confirm each Third Party's receipt of the instructions required by Subsection A above. Defendant must provide all receipts of confirmation and any responses from Third Parties within five (5) days of receipt to: DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "United States v. Easy Healthcare Corporation."

D. Defendant shall not use any Third Party identified in Subsection A above to advertise, market, promote, offer, offer for sale, or sell any product or service until Defendant confirm each Third Party's receipt of the instructions required by Subsection A above.

VII. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that any Covered Business, in connection with the collection, maintenance, use, disclosure of, or provision of access to, Covered Information, must, within sixty (60) days of entry of this Order, establish and implement, and thereafter maintain, a comprehensive privacy and information security program ("Program") that protects the privacy, security, availability, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Defendant must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written program and any evaluations thereof or updates thereto to each Covered Business's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Covered Business responsible for the Covered Business's Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

C. Designate a qualified employee or employees, who report(s) directly to the Chief Executive Officer(s) or, in the event a Chief Executive Officer role does not exist, a similarly-situated executive, to coordinate and be responsible for the Program; and keep the Chief Executive Officer(s) and Board of Directors informed of the Program, including all actions and procedures implemented to comply with the requirements of this Order, and any actions and procedures to be implemented to ensure continued compliance with this Order;

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks in each area of the Covered Business's operations to the privacy, security, availability, confidentiality, and integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of, or provision of access to, Covered Information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks to the privacy, security, availability, confidentiality, and integrity of Covered Information identified by each Covered Business in response to Subsection VII.D. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, disclosure of, or provision of access to, the Covered Information. Such safeguards must also include:

1. policies, procedures, and technical measures to systematically inventory Covered Information in the Covered Business's control and delete Covered Information that is no longer necessary to fulfill the purpose for which the Covered Information was collected;

2. policies, procedures, and technical measures to prevent the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information inconsistent with the Covered Business's representations to consumers;

3. audits, assessments, and reviews of the contracts, privacy policies, and terms of service associated with any Third Party to which each Covered Business discloses or provides access to Covered Information;

4. policies, procedures, and controls to ensure the Covered Business complies with Sections I-IV above;

5. policies and technical measures that limit employee and contractor access to Covered Information to only those employees and contractors with a legitimate business need to access such Covered Information;

6. mandatory privacy training programs for all employees on at least an annual basis, updated to address the collection, use, and disclosure of Covered Information; any internal or external risks identified by each Covered Business in Subsection VII.D and safeguards implemented pursuant to Subsection VII.E, that includes training on the requirements of this Order;

7. a data retention policy that, at a minimum, includes

   a. a retention schedule that limits the retention of Covered Information for only as long as is reasonably necessary to fulfill the purpose for which the Covered Information was collected; provided, however, that such Covered Information need not be destroyed, and may be disclosed, to the extent requested by a government agency or required by law, regulation, or court order; and

   b. a requirement that each Covered Business document, adhere to, and make publicly available in its privacy policy a retention schedule for Covered Information, setting forth: (1) the purposes for which such information is collected; (2) the specific business need for retaining each type of Covered Information; and (3) a set timeframe for deletion of each type of Covered Information

(absent any intervening deletion requests from consumers) that precludes indefinite retention of any such Covered Information;

8. audits, assessments, reviews, or testing of Software Development Kits, and their associated Third Parties, to which each Covered Business shares or provides access to Covered Information of any Covered User; and

9. For each product or service offered by any Covered Business, Clearly and Conspicuously disclose the categories of Covered Information collected from Covered Users, the purposes for the collection of each category of such Covered Information, and any transfers of such Covered Information to Third Parties. For each such transfer of Covered Information, such disclosure must, at a minimum, include

a. the specific categories of Covered Information transferred;

b. the identity and specific category of the recipient Third Party of each such transfer;

c. the purposes for which the Covered Business transferred the Covered Information; and

d. the purposes for which each recipient Third Party of Covered Information could use such Covered Information, including but not limited to the purposes for which each recipient reserves the right to use such Covered Information; and

e. whether each recipient Third Party of such transfer of Covered Information reserves the right to transfer such Covered Information to other parties.

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, availability, confidentiality, and integrity of Covered Information, and modify the Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Program based on the results;

H. Select and retain service providers capable of safeguarding Covered Information it receives from the Covered Business, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, availability, confidentiality, or integrity of Covered Information;

I. Evaluate and adjust the Program in light of any material changes to each Covered Business's operations or business arrangements, the results of the testing and monitoring required by Subsection VII.F, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Subsection VII.D, and any other circumstances that the Covered Business knows or has reason to believe may have a material impact on the effectiveness of the Program or any of its individual safeguards. The Covered Business may make this evaluation and adjustment to the Program at any time, but must, at a minimum, evaluate the Program at least once every twelve (12) months and modify the Program as necessary based on the results.

VIII. PRIVACY AND INFORMATION SECURITY ASSESSMENT BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Section VII, for any Covered Business that collects, maintains, uses, discloses, or provides access to Covered Information, Defendant must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)") who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Program; (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim. Defendant may obtain separate assessments for: (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above. The Assessor(s) must have a minimum of three (3) years of experience in the field of privacy and data protection.

B. For each Assessment, Defendant must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in his or her sole discretion.

C. The reporting period for the Assessments must cover: (1) the first one-hundred-and-eighty (180) days after the Privacy and Information Security Program required by Section

VII has been put in place for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after the entry of this Order for the biennial Assessment.

D. Each Assessment must, for the entire assessment period:

1. determine whether Defendant has implemented and maintained the Program required by Section VII;

2. assess the effectiveness of Defendant's implementation and maintenance of Subsections VII.A-I;

3. identify any gaps or weaknesses in the Program or instances of material noncompliance with Subsections VII.A-I;

4. address the status of gaps or weaknesses in the Program, as well as any instances of material non-compliance with Subsections VII.A-I, that were identified in any prior Assessment required by this Order; and

5. identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Defendant's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Defendant, Defendant's management, or a Covered Business's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely solely on assertions or attestations by Defendant, Defendant's management or a Covered Business's management and state the number of hours that each member of the Assessor's assessment team worked on the Assessment. To the extent Defendant revises, updates, or adds one or more safeguards required

under Section VII.E in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within ninety (90) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Defendant must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "United States v. Easy Healthcare Corporation." All subsequent biennial Assessments must be retained by Defendant until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IX. COOPERATION WITH ASSESSOR(S)

IT IS FURTHER ORDERED that Defendant, whether acting directly or indirectly, in connection with the Assessments required by Section VIII, must:

A. Provide or otherwise make available to the Assessor(s) all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor(s) information about all Covered Information in Defendant's custody or control that is relevant to the Assessment, so that the Assessor(s) can determine the scope of the Assessment; and

C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Defendant has implemented and maintained the Program required by Section VII; (2) assessment of the effectiveness of the implementation and maintenance of Subsections VII.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program required by Section VII.

X. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that Defendant must:

A. One (1) year after the entry of this Order, and each year thereafter for twenty (20) years, provide the Commission with a certification from Defendant, for each Covered Business, that: (1) the Covered Business has established, implemented, and maintained the requirements of this Order; (2) the Covered Business is not aware of any material noncompliance that has not been: (a) corrected, or (b) disclosed to the Commission; and (3) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin, "United States v. Easy Healthcare Corporation."

XI. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Defendant, for any Covered Business, within thirty (30) days after Defendant's discovery of a Covered Incident, must submit a report to the Commission, unless the Covered Incident also constitutes a Breach of Security involving the Unsecured PHR Identifiable Health Information of 500 or more individuals and therefore requiring notice under Section IV of this Order. The report must include, to the extent possible:

A. the date, estimated date, or estimated date range when the Covered Incident occurred;

B. a description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

C. the number of consumers whose information was affected;

D. the acts that Defendant has taken to date to remediate the Covered Incident; protect Covered Information from further disclosure, exposure, or access; and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

E. a representative copy of any materially different notice sent by Defendant to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "United States v. Easy Healthcare Corporation."

XII. MONETARY JUDGMENT FOR CIVIL PENALTY

IT IS FURTHER ORDERED that:

A. Judgment in the amount of one hundred thousand Dollars ($100,000) is entered in favor of Plaintiff against Defendant, jointly and severally, as a civil penalty.

B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the United States, one hundred thousand Dollars ($100,000), which, as Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment to Plaintiff. Such payment must be made within seven (7) days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of Plaintiff.

XIII. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

A. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission in a proceeding to enforce its rights to any payment or monetary judgment pursuant to this Order.

C. Defendant acknowledges that their Taxpayer Identification Numbers, Social Security Numbers, or Employer Identification Numbers, which Defendant previously submitted to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. §7701.

XIV. ORDER ACKNOWLEDGEMENTS

IT IS FURTHER ORDERED that Defendant obtains acknowledgments of receipt of this Order:

A. Defendant, within seven (7) days after the entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For twenty (20) years after entry of this Order, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives having managerial responsibilities for conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Section titled Compliance Reporting. Delivery must occur within fourteen (14) days after entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Defendant delivered a copy of this Order, Defendant must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XV. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Defendant makes timely submissions to the Commission:

A. One year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury. Defendant must:

1. identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission and Plaintiff may use to communicate with Defendant;

2. identify all of Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses;

3. describe the activities of each business, including the products and services offered, the means of advertising, marketing, and sales, and the involvement of Defendant;

4. describe in detail whether and how Defendant is in compliance with each

Section of this Order; and

5. provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

B. For twenty (20) years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following:

1. Any designated point of contact; or

2. The structure of Defendant or any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Defendant within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "United States v. Easy Healthcare Corporation."

XVI. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for twenty

(20) years after the entry of the Order, and retain each such record for five (5) years, unless otherwise specified below. Specifically, Defendant for any business that Defendant is a majority owner or controls directly or indirectly must create and retain the following records:

A. accounting records showing the revenues from all products or services sold;

B. personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. copies or records of all consumer complaints and refund requests related to any mobile application or website offered by Defendant, concerning the collection, use, maintenance, disclosure, deletion, or permission of access to Covered Information, whether received directly or indirectly, such as through a third party, and any response;

D. records of all disclosures of Health Information or PHR Identifiable Health Information to Third Parties showing, for each Third Party that received Health Information or PHR Identifiable Health Information, the name and address of the Third Party, the date(s) of such disclosures, the purpose(s) for which the Health Information or PHR Identifiable Health Information was transferred, and how and when Covered Users provided authorization for the disclosures;

D. records of all disclosures of App Events to Third Parties;

E. a copy of each unique advertisement, form advertisement (where an advertisement is generated based on a form advertisement), or other marketing material making a representation subject to this Order;

G. a copy of each widely disseminated representation by Defendant that describes

the extent to which Defendant maintains or protects the privacy, security, and confidentiality of any Covered Information, including any representation concerning a change in any website or other service controlled by Defendant that relates to the privacy, security, and confidentiality of Covered Information;

H. for five (5) years after the date of preparation of each Assessment required by Section VIII, all materials provided to the Assessor(s) by the Respondent to prepare the Assessment, whether prepared by or on behalf of Defendant, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Defendant's compliance with related Sections of this Order, for the compliance period covered by such Assessment;

I. for five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communication relate to Defendant's compliance with this Order;

J. for five (5) years from the date created or received, all records, whether prepared by or on behalf of Defendant, that tend to show any lack of compliance by Defendant with this Order; and

K. all records necessary to demonstrate full compliance with each section of this Order, including all submissions to the Commission.

XVII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission or Plaintiff, Defendant must: submit additional compliance reports or other

requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying. The Commission and Plaintiff are also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission and Plaintiff are authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission and Plaintiff to interview anyone affiliated with Defendant who has agreed to such an interview. The person interviewed may have counsel present.

C. The Commission and Plaintiff may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XVIII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

SO ORDERED this ___ day of _____, 20__

_____
UNITED STATES DISTRICT JUDGE

SO STIPULATED AND AGREED:

FOR PLAINTIFF UNITED STATES OF AMERICA

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorney General

AMANDA N. LISKAMM
Director

LISA K. HSIAO
Assistant Director

/s/ *Rachel E. Baron*
RACHEL E. BARON
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
Civil Division
450 Fifth Street NW
Washington, D.C. 20530
(202) 598-7719

OF COUNSEL

FOR THE FEDERAL TRADE COMMISSION

TIFFANY GEORGE
Acting Assistant Director
Division of Privacy and Identity Protection

DAVID WALKO
RONNIE SOLOMON
Attorneys
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
(202) 326-2880
(202) 326-2098
dwalko@ftc.gov
rsolomon@ftc.gov

FOR DEFENDANT EASY HEALTHCARE CORPORATION:

Brenda Sharton

Date: 3/24/2023

Brenda R. Sharton
Benjamin M. Sadun
Hilary Bonaccorsi
DECHERT LLP

Counsel for Easy Healthcare Corporation

DEFENDANT:

XIAOLIAN LIU

Date: 03/27/2023

Xiaolian Liu
Chief Executive Officer
Easy Healthcare Corporation

Exhibit A

[To appear with the Easy Healthcare logo]
Website and Mobile Application Notice

Between November 2017 and August 2022, we shared the personal information (such as unique identification number) of users of the Premom Ovulation Tracker app with the analytics divisions of Google and AppsFlyer. We also shared activities on the app related to users' fertility, periods, and pregnancy. Between January 2018 and August 2020, we also shared users' information with Aurora Mobile and Umeng. This included the unique identification number from users' phones and their device location.

We did not share users' names, birth dates, or addresses with any of the above companies.

The Federal Trade Commission alleged that we shared this information without users' permission in violation of the law. To resolve the case with the FTC,

- We'll tell Google and AppsFlyer to delete the information that the FTC says we collected without our users' permission. And we'll tell Aurora Mobile and Umeng to delete all information that the FTC says we collected without our users' permission, too.
- We'll never share your health information with third parties (like Google, AppsFlyer, Aurora Mobile, or Umeng) for advertising purposes.
- We won't share your health information with third parties (like Google, AppsFlyer, Aurora Mobile, or Umeng) for other purposes, unless we get your permission first.
- We'll put in place a comprehensive privacy and information security program to protect our users' information. An independent auditor will review our program to make sure we are protecting our users' information. These audits will happen every two years for 20 years.

If you have any questions, you can email us at [email]@premom.com.

To learn more about the settlement, go to ftc.gov and search for "Premom".

Read the FTC's Does your health app protect your sensitive info? to learn more about protecting your health privacy.

Notice to Covered Users

Between November 2017 and August 2022, you used the Premom Ovulation Tracker app. During that time, we shared your information (such as unique identification number) with the analytics divisions of Google and AppsFlyer. We also shared activities on the app related to your fertility, periods, and pregnancy. If you used the Premom Ovulation Tracker app between January 2018 and August 2020, we also shared your information with Aurora Mobile and Umeng. This included the unique identification number from your phone and your device location.

We did not share your name, birth date, or address with any of these companies.

The Federal Trade Commission alleged that we shared this information without users' permission in violation of the law. To resolve the case with the FTC,

- We'll tell Google and AppsFlyer to delete the information that the FTC says we collected without our users' permission. And we'll tell Aurora Mobile and Umeng to delete all information that the FTC says we collected without our users' permission, too.
- We'll never share your health information with third parties (like Google, AppsFlyer, Aurora Mobile, or Umeng) for advertising purposes.
- We won't share your health information with third parties (like Google, AppsFlyer, Aurora Mobile, or Umeng) for other purposes, unless we get your permission first.
- We'll put in place a comprehensive privacy and information security program to protect your information. An independent auditor will review our program to make sure we are protecting your information. These audits will happen every two years for 20 years.

If you have any questions, you can email us at [email]@premom.com.

To learn more about the settlement, go to ftc.gov and search for "Premom".

Read the FTC's Does your health app protect your sensitive info? to learn more about protecting your health privacy.