EU PRIVACY & SECURITY POLICIES AND PROCEDURES

Table of Contents

PRIVACY & SECURITY POLICIES IN GENERAL AND DEFINITIONS 4

1. General 4

2. Definitions 4

PRIVACY AND SECURITY OFFICER RESPONSIBILITIES 5

3. Privacy and Security Officer 5

WORKFORCE RESPONSIBILITIES, ACCESS TO PHI, TRAINING, SANCTIONS, AND NO RETALIATION 6

4. General 6

5. Assessing/Granting Workforce Access to PHI 8

6. Training 8

7. Enforcement and Sanctions 8

8. No Intimidation or Retaliation 9

SYSTEMS AND WORKSPACE SECURITY 9

9. General 9

10. Use of Electronic Portable Devices 9

11. Visitors 9

12. Treatment of Communications of Personal Data 9

13. Copy Machines and Copying Services 9

RISK ASSESSMENTS AND MANAGEMENT, INVESTIGATIONS, AUDITS, TESTING OF ELECTRONIC SYSTEMS, AND DOCUMENTATION 10

14. Ongoing Assessments 10

ACCESS TO AND DISCLOSURE OF PERSONAL DATA TO PERSONS AND ENTITIES ACTING ON HEARTFLOW'S BEHALF OR PERFORMING SERVICES UNDER CONTRACT WITH HEARTFLOW 11

15. Providers, Vendors, and Others Not Part of Workforce 11

16. HeartFlow's Notice of Privacy Practices ("NPP") 11

17. Request from Patients in relation to Personal Data 12

18. Record Retention 13

19. Complaints 13

20. Reporting Security Incidents and/or Breaches 14

PRIVACY & SECURITY POLICIES IN GENERAL AND DEFINITIONS

1. **General**

1.1 These Policies and Procedures concerning Personal Data collected in the European Union ("EU") are supplemental to Heartflow's Privacy & Security Procedures and apply to Heartflow's collection of personal data (as defined herein) in the EU and are, and at all times will be, based on Privacy Laws and on the risk assessments, audits, and monitoring performed by HeartFlow.

1.2 HeartFlow will not access, use, disclose, modify, or destroy personal data in its possession in a manner inconsistent with these Policies and Procedures and/or with applicable Privacy Laws.

1.3 HeartFlow will at all times safeguard and protect the privacy and security of personal data in accordance with applicable Privacy Laws.

1.4 HeartFlow will provide patients and their representatives with appropriate access to personal data in accordance with Privacy Laws.

1.5 HeartFlow will continue to conduct risk assessments and monitor compliance with applicable Privacy Laws as required to protect the confidentiality, integrity, and availability of personal data, and will revise these Policies and Procedures as necessary to ensure compliance with Privacy Laws and best practices.

1.6 HeartFlow's executive team will timely approve, adopt and implement these Policies and Procedures, and any modifications or amendments as may be necessitated by Privacy Laws, material changes in operations, technology, and/or legal regulations or guidance.

2. **Definitions**

2.1 Capitalizations. Capitalized terms in these Policies and Procedures, and any subsequent policies adopted by HeartFlow related to applicable Privacy Laws, have the definitions given them under privacy laws as set forth herein.

2.2 Electronic Portable Device. An "Electronic Portable Device" is any portable or mobile device made available to, or otherwise owned or used by, Workforce Members, as defined below, that can be used to transmit or store personal data, including, but not limited to, laptops, tablets, smart phones, cell phones, compact disks, thumb drives, and laptops, Personal Digital Assistants (PDAs), palmtop computers, portable/handheld telecommunications devices (e.g., cellular telephones, pagers, and radios), cameras (both digital and analog), and other similar devices and specifically applies to any handheld device that makes or receives phone calls, leaves messages, sends text messages, browses the Internet, or downloads and allows for the reading of and responding to emails.

2.3 Health-care Provider. The EU based provider of treatment to a Patient which is the Data Controller.

2.4 HeartFlow-Provided Device. Any device, including desktop or laptop computers and mobile devices or phones, including an Electronic Portable Device, provided to Workforce Members by HeartFlow for work-related purposes (e.g., when a Workforce Member is engaging in HeartFlow

business or otherwise performing an activity for the benefit of HeartFlow and is authorized to perform such task/activity by HeartFlow as part of their job description).

2.5 HeartFlow Privacy & Security Policies and Procedures. The Privacy & Security Policies and Procedures which govern HeartFlow's Privacy & Security Practices

2.6 Patient. "Patient" refers to individuals who have been the subject of a HeartFlow Analysis as a patient of a physician providing treatment via a HeartFlow provider/customer. "Patient" also includes such individuals' authorized representative(s).

2.7 Personal Devices. "Personal Devices" are any devices, including Electronic Portable Devices, owned and maintained by or personal to a Workforce Member and not provided by HeartFlow.

2.8 Personal Data. "Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person and includes, without limitation, generic data and data concerning the health (as defined in applicable Privacy Laws) of a natural person.

2.9 Processing. "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and "process" shall be construed accordingly.

2.10 Workforce Members or Workforce. A "Workforce Member" is any HeartFlow officer, executive, director, employee, volunteer, trainee, or other personnel, including an independent contractor performing work for or on behalf of HeartFlow that involves Personal Data and/or whose conduct, in the performance of work for HeartFlow, is under the direct control of HeartFlow, whether or not he or she is paid by HeartFlow and regardless of their job classification, including the Privacy Officer. "Workforce" refers to the collective Workforce Members.

2.11 Workspace. A "Workspace" is any physical space where Workforce Members perform their job duties and/or where HeartFlow's information systems are housed or located.

2.12 Work Station. A "Work Station" is any station within the Workspace where Workforce may physically and/or electronically access HeartFlow's information system including, but not limited to, Personal Data, electronic health records, and onsite and offsite backup systems.

PRIVACY AND SECURITY OFFICER RESPONSIBILITIES

3. Privacy and Security Officer

3.1 In furtherance of the policies described herein, and specifically to effectively implement, manage, and maintain programing to ensure ongoing compliance with Privacy Laws throughout the organization, Heartflow has appointed a Privacy Officer and a Security Officer (collectively, "Officers" or "Officer" for either or each of them). The role and responsibility of the Officers is

governed by HeartFlow's Privacy & Security Policies and Procedures. All queries related to the collection or use of personal data should be directed to the Officers and will be managed in accordance with the roles and responsibilities of the Officers as set out in HeartFlow's Privacy & Security Policies and Procedures.

WORKFORCE RESPONSIBILITIES, ACCESS TO PHI, TRAINING, SANCTIONS, AND NO RETALIATION

4. **General**

4.1 HeartFlow understands that the success of its efforts to comply with Privacy Laws depends on the commitment, integrity, and performance of each Workforce Member. Accordingly, HeartFlow requires that each and every Workforce Member complies at all times with these Policies and Procedures and applicable Privacy Laws and performs such further actions as directed by Officer(s) or their designees hereunder.

4.2 Heartflow-provided Devices and Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, corporate cloud services (Google Apps, Workday, etc.), network accounts providing electronic mail, internet browsing, and FTP, are to be used only for business purposes serving the interests of the company and its clients and customers in the course of normal operations.

4.3 Workforce must, at all times, protect and safeguard Personal Data from unauthorized access, use, disclosure and/or destruction. Providing any system or user access to any unauthorized individual, either deliberately or through failure to secure its access, is strictly prohibited.

4.4 In addition to the other privacy and security protocols and procedures described herein, Workforce Members will take responsibility for ensuring that physical security measures are maintained by each of them.

4.5 Workforce shall also secure all Personal Data and/or other sensitive or proprietary information as follows:

(a) Keeping hard copies of documents (paper copies) containing Personal Data covered or otherwise out of plain view from unauthorized persons passing by, especially visitors, and, when leaving an area where such information is being used or viewed, locking such documents in secure, designated areas;
(b) Moving computer monitors or other electronic media with visible screens in a way that keeps Personal Data exposed or otherwise obscuring information on the screen when unauthorized persons, especially visitors, pass by;
(c) Never leaving Personal Data unattended or available on printers, copiers, and fax machines, but instead, always locking them in drawers or storage areas or at a minimum, removing them from plain sight;
(d) Never using photocopiers and other reproduction technology (such as scanners and digital cameras) to copy Personal Data without a legitimate business reason;
(e) Disposing of and/or destroying Personal Data only when authorized to do so and only by placing in secure shred bins;

(f) Locking computer screens when leaving workspaces to ensure no unauthorized information can be viewed.

(g) Logging off from any sessions to web applications, databases, or other confidential applications when finished and not keeping inactive/unused sessions active.

4.6 Workforce Members must have a legitimate business reason to discuss Personal Data orally with other Workforce Members, persons who are the subject of the Personal Data, health plans or other payers, whether electronically, on the telephone or in person. Workforce members may not discuss Personal Data outside HeartFlow in the presence of persons who are not authorized to access the Personal Data or who have no legitimate business reason to hear the discussion. When discussing Personal Data within HeartFlow premises, Workforce members must make reasonable efforts to ensure that other Workforce Members and persons who do not have a legitimate business reason to hear the Personal Data cannot hear the discussion or are not likely to retain the information.

4.7 Workforce Members are encouraged to notify the Privacy or Security Officer(s) whenever they believe that these Policies and Procedures should be modified or amended to maintain compliance with applicable Privacy Laws, when they do not understand some aspect of the Policies or Privacy Laws or have questions, and when they suspect a violation has occurred. Workforce Members may report anonymously through HeartFlow's Ethics Compliance Hotline or may submit their questions and/or reports to the Chief Ethics & Compliance Officer, Privacy Officer, Security Officer, their manager, HR, any member of the executive staff, or the General Counsel.

4.8 Workforce Members may access personal email accounts while logged-on to HeartFlow's information system to a reasonable extent during work hours. However, Workforce Members shall take precautions so as not to download email attachments or enclosures from unknown senders, follow links, or take other actions that may allow malware, viruses, email bombs, etc. to jeopardize the integrity of Heartflow's data systems, and must take all possible precautions to protect against any threat to the integrity and security of Personal Data.

4.9 Absent approval from HeartFlow's Privacy Officer and/or Security Officer, Workforce Members may not access social media accounts (e.g., Facebook, Twitter) from a HeartFlow Work Station. Further, Workforce Member may not access any HeartFlow data, a HeartFlow server, or any HeartFlow application account for any purpose during business hours other than to conduct HeartFlow business.

4.10 HeartFlow reserves the right to audit and monitor all networks, systems, communications, activity and records of and relating to Workforce use of HeartFlow-Provided Devices and/or Personal Devices at any and all times to ensure compliance with these Policies and Procedures and law, including activity on Personal Devices used at any time for HeartFlow-related work or conduct. Workforce Members will have no expectation of privacy regarding such communications or records.

5. **Assessing/Granting Workforce Access to PHI**

5.1 Privacy and Security Officers will ensure that all candidates for employment, contractors, third party users, Workforce Members and others who will or may require Personal Data access to legitimately perform their job functions are subject to appropriate background checks prior to conducting any job duties that access Personal Data, in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Factors such as those Workforce Members who require Personal Data access to legitimately perform their individual job functions how Personal Data is accessed are governed by Heartflow's Privacy & Security Procedures.

6. **Training**

6.1 The Workforce will receive training regarding these Policies and Procedures and applicable Privacy Laws at least at the following times:

(a) Prior to being granted access to Personal Data;
(b) Upon applicable changes to Privacy Laws;
(c) Upon implementing a material change to these Policies and Procedures;
(d) When a Workforce Member's duties or functions change, or are otherwise affected by changes to these Policies and Procedures;
(e) As determined appropriate by Privacy or Security Officer(s), such as if a Security Incident or Breach occurs; and/or
(f) Annually, if Privacy or Security Officers determine annual training is appropriate or necessary to ensure compliance.

6.2 The Privacy Officer will continually evaluate, monitor and update HeartFlow's Workforce training program and materials, including reminding Workforce through alerts, bulletins, and other methods, including face-to-face discussions, about the appropriate use of laptops and other field devices, email communications, overall patient confidentiality, etc., and regarding potential and/or actual compromises of Personal Data, Security Incidents and/or Breaches.

6.3 Further detail about training, including content and frequency is set out in Heartflow's Privacy & Security Procedures.

7. **Enforcement and Sanctions**

7.1 Privacy and Security Officers will monitor and/or audit Workforce conduct as appropriate to support and enforce compliance with these Policies and Procedures and with Privacy Laws.

7.2 When a Workforce Member violates these Policies or Procedures or Privacy Laws, the Privacy Officer, in consultation with the Chief Ethics & Compliance Officer, Human Resources, management and/or legal professionals, as appropriate, will determine what sanctions should be imposed on the Workforce Member. Workforce Members will be sanctioned according to the severity of the violation as follows:

(a) Minor or unrepeated violations will result in brief counseling and, if necessary, additional privacy and/or security training.

(b) A pattern of repeated, significant violations may be grounds for suspension or termination.

(c) A deliberate violation will result in immediate suspension and the termination of all access to Personal Data and information resources and may result in termination of employment.

7.3 The Privacy Officer will record any sanctions imposed on Workforce Members, and documentation will be retained in the Workforce Member's personnel record.

8. **No Intimidation or Retaliation**

8.1 HeartFlow will not intimidate, threaten, coerce, discriminate, retaliate, or withhold treatment from any Workforce Member or other individual for exercising any rights under Privacy Laws, including submitting complaints, filing reports, etc. Any Workforce Member who violates this non-intimidation or retaliation policy will be sanctioned as described in these Policies and Procedures.

8.2 Workforce Members must notify the General Counsel, Chief Ethics & Compliance Officer, Privacy Officer or HeartFlow's outside legal counsel of any retaliatory act or intimidation.

SYSTEMS AND WORKSPACE SECURITY

9. **General**

9.1 Full details about Heartflow's Systems and Workplace Security are set out in Heartflow's Privacy and Security Policies and Procedures and must be observed at all times by Workforce Members.

10. **Use of Electronic Portable Devices**

10.1 Full details about Heartflow's policy on the use of Personal Devices are set out in Heartflow's Privacy and Security Policies and Procedures and must be observed at all times by Workforce Members.

11. **Visitors**

11.1 All persons visiting the Workspace who are not Workforce Members must be supervised by a Workforce Member to assure that the visitor will be prevented from viewing, accessing, and/or retaining any Personal Data, and will comply with all requests and/or instructions from Security or Privacy Officers.

12. **Treatment of Communications of Personal Data**

12.1 Full details about Heartflow's policy on the transmission of Personal Data via Telephone, Email, Web applications, in paper and by Fax are set out in Heartflow's Privacy and Security Policies and Procedures and must be observed at all times by Workforce Members.

13. **Copy Machines and Copying Services**

13.1 Personal Data will not be left unattended on HeartFlow's copy machines.

13.2 Personal Data will not be sent out to a copying service unless HeartFlow's existing copying abilities cannot accommodate the job, in which case HeartFlow must have a data processing agreement in a form which is compliant with applicable Privacy Laws with the copying service and must ensure appropriate safeguards are used during the transport and delivery of Personal Data to and from the copy service.

RISK ASSESSMENTS AND MANAGEMENT, INVESTIGATIONS, AUDITS, TESTING OF ELECTRONIC SYSTEMS, AND DOCUMENTATION

14. Ongoing Assessments

14.1 On an ongoing basis as appropriate to comply with Privacy Laws, the Privacy Officer will assess and monitor any potential and actual risks or vulnerabilities to the confidentiality, integrity, and availability of Personal Data ("Ongoing Assessments"), including:

(a) Monitoring, auditing, or evaluating Workforce operations, practices, uses, and disclosures of Personal Data to ensure Workforce's compliance with these Policies and Procedures;
(b) Ensuring that these Policies and Procedures are effective and work well with HeartFlow operations;
(c) Identifying HeartFlow processes that may result in the unauthorized access, use, or disclosure of Personal Data, Security Incidents, and/or Breaches;
(d) Identifying practices and processes to mitigate any actual or potential risks of the unauthorized access, use, or disclosure of Personal Data, or other Security Incidents, and/or Breaches;
(e) Promptly responding to reports of actual or potential unauthorized disclosures of Personal Data, Security Incidents, and/or Breaches and complying with all applicable Privacy Laws; and
(f) Monitoring, auditing, or evaluating subcontractors, or other third party vendor practices, uses or disclosures of Personal Data to ensure compliance with these Policies and Procedures and Privacy Laws.

14.2 Ongoing Assessments and related activities will be documented and maintained in accordance with the document retention provisions of Heartflow's Privacy & Security Policies and Procedures.

14.3 In consultation with legal counsel, as appropriate, Privacy Officer will make any necessary modifications to these Policies and Procedures, ensure they are properly approved by company leadership, notify Workforce Members, and offer related training as appropriate.

ACCESS TO AND DISCLOSURE OF PERSONAL DATA TO PERSONS AND ENTITIES ACTING ON HEARTFLOW'S BEHALF OR PERFORMING SERVICES UNDER CONTRACT WITH HEARTFLOW

15. **Providers, Vendors, and Others Not Part of Workforce**

15.1 Privacy Laws require that providers and vendors (sub-processors) enter into written agreements with us if, as part of the service they provide to us, they process Personal Data on our behalf. Privacy Officer will determine whether a data processing agreement is required or prudent under the circumstances, and if so, will ensure that Heartflow enters into such an agreement with such persons or entities before HeartFlow provides Personal Data to such entity. Put differently, HeartFlow may allow entities performing services to, for, or on behalf of HeartFlow to access, use, maintain, transmit, and/or create Personal Data without Patient authorization only if HeartFlow and such person or entity have entered a written data processing agreement which is compliant with applicable Privacy Laws.

15.2 Privacy Officer will perform background checks on sub-processors.

15.3 Workforce who become aware of sub-processors who may have access to Personal Data must not provide access to Personal Data under any circumstances without first confirming with Privacy Officer that such persons or entities have valid, current, executed data processing agreements and/or confidentiality agreements with HeartFlow, as appropriate. If such information cannot be determined, or if there is any question about the validity of such agreements, then Workforce must not provide any access whatsoever to such persons or entities unless and until permission is provided through the office of the General Counsel.

15.4 Privacy Officer will create and maintain an inventory of all existing data processing agreements and Confidentiality Agreements, describing the terms of termination thereof or the date on which each data processing agreement and/or Confidentiality Agreement will terminate, and will retain the original(s) for ten (10) years following termination of the data processing agreements or Confidentiality Agreement.

16. **HeartFlow's Notice of Privacy Practices ("NPP")**

16.1 HeartFlow acknowledges that individuals have a fundamental right to be informed of its privacy practices and of their privacy rights with respect to their Personal Data. HeartFlow has developed an Privacy Notice applicable in the EU that is designed to provide information, in clear and plain language, to individuals on privacy issues and concerns in accordance with applicable Privacy Laws.

16.2 Workforce Members will make a copy of the posted Privacy Notice available upon the request of any person who asks for it. Workforce Members may e-mail the NPP to an individual based on the procedures set forth below

(a) The Workforce Member may email the Privacy Notice to the requesting individual if the individual agrees to receive an electronic notice and such agreement has not been withdrawn.

(b) The Workforce Member must email the electronic Privacy Notice as soon as reasonably practicable.

(c) If the Workforce Member knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual.

(d) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

16.3 HeartFlow will revise its NPP whenever there is a material change to the uses for Personal Data or to whom it is disclosed, or other privacy practices stated in the NPP. Except when required by law, a material change to any term of the NPP will not be implemented prior to the effective date of the notice in which such material change is reflected.

16.4 HeartFlow will document and maintain copies of all versions of its NPPs.

17. **Request from Patients in relation to Personal Data**

17.1 HeartFlow recognizes that every Patient has certain rights under Privacy Laws in relation to the Personal Data we hold about them. Unless limited by applicable Privacy Laws, HeartFlow will provide reasonable assistance to the Health-Care Provider to ensure that requests made by Patients to the relevant Health-Care Provider, as the Data Controller, are complied with in accordance with Privacy Laws.

17.2 Relevant requests from Patients under Privacy Laws include, but are not limited to requests for access to Personal Data, requests for modification of Personal Data and requests for deletion of Personal Data.

17.3 In case of a request for Personal Data, if the requested Personal Data is not retained by HeartFlow, HeartFlow will direct the Health-Care Provider to the provider, individual, or entity that maintains the Personal Data, if known.

17.4 All requests received which relate to a Patient exercising his or her rights in respect of the Personal Data HeartFlow holds must be referred to the Privacy Officer who is responsible for determining whether the request will be granted and will inform the Health-Care Provider the decision and, if not granted, the reason for refusing.

17.5 In response to requests from Patients to requests for access to and copies of a patient's Personal Data, Workforce Members will ensure the validity of the request by making all necessary and appropriate checks with the relevant Health-Care Provider.

17.6 If a Patient's request for a copy of Personal Data is approved or HeartFlow agrees to a summary or explanation of such information, HeartFlow may impose a reasonable fee (to be met by the Health-Care Provider) as a condition of receiving Personal Data, provided that the fee includes **only** the cost of:

(a) Copying, including the cost of supplies for, but not the labor associated with, copying the Personal Data requested, not to exceed £0.25 pence per page or £0.50 pence for records that are copied from microfilm or another similar medium;

(b) Postage when the individual has requested the copy, summary, or explanation be mailed; and

(c) Preparing an explanation or summary of the Personal Data, if agreed to by the individual.

18. **Record Retention**

18.1 HeartFlow will retain Patients' Personal Data for such period as to ensure compliance applicable Privacy Laws.

19. **International Data Transfers**

19.1 HeartFlow may transfer personal information to outside the European Economic Area (EEA) to our Group Company in the United States of America on the basis that our Group Company receiving the information has provided adequate safeguards by way of standard data protection clauses.

20. **Complaints**

20.1 Patients may submit complaints to HeartFlow regarding the use or disclosure of Personal Data. Such complaints must be directed or submitted to Privacy Officer.

20.2 Privacy Officer will document the complaints in consultation with and at the direction of legal counsel.

20.3 Privacy Officer will review all applicable information related to the use or disclosure of the Patient's Personal Data that is the subject of the complaint(s), in consultation with and at the direction of legal counsel.

20.4 At the direction of legal counsel, Privacy Officer will review all complaints within fourteen (14) days of receipt. If the complaint requires a response, and contact information is provided, Privacy Officer or designee will prepare and deliver a written response to the Patient. If the complaint does not require a response or contact information is not provided, Privacy Officer or designee will prepare a written statement of any action taken and attach it to the filed complaint.

20.5 If a use or disclosure violation is confirmed, Privacy Officer, in consultation with legal counsel as appropriate, will sanction the Workforce Member responsible, if applicable, based on facts and circumstances, including factors such as the severity of the violation, whether it was intentional or unintentional, and whether the violation indicates a pattern of improper use, disclosure or release of Personal Data and/or misuse of computing resources. Privacy Officer will document the actions taken and place all information relating to the complaint in HeartFlow's files.

20.6 If Privacy Officer, in consultation with legal counsel, determines that the complaint has no merit, the investigation will be documented and placed in HeartFlow's file.

20.7 At no time will a Workforce Member who is the subject of a complaint be the same person responsible for investigating the complaint.

20.8 In the event that the complaint is about Privacy Officer, legal counsel will be notified and will investigate, or direct investigation of, the complaint.

21. **Reporting Security Incidents and/or Breaches**

21.1 Either Privacy and/or Security Officer will immediately or as soon as practicable analyze and respond to reports, complaints, Security Incidents, and Breaches, and will promptly communicate Reportable Incidents to HeartFlow's legal counsel and, as directed by legal counsel to maintain the attorney-client privilege and work product protection.

21.2 HeartFlow will provide the Health-Care Provider without undue delay with such details as it requires regarding the nature of any Personal Data Breach (including the categories and approximate numbers of individuals affected and records concerned), information concerning any investigations into such breach, the likely consequences of the Personal Data Breach and any measures it has taken, or intends to take to mitigate its possible adverse effects.

21.3 HeartFlow, in consultation with legal counsel, will ensure that where HeartFlow is required by Privacy Laws and/or contract to give notice of any Security Incident or Breach, such notifications are made in the form and timeframe as required by Privacy Laws, contract, and HeartFlow's Security Incident and Breach Policies and Procedures. Specifically, Officers will determine the time within which reporting must occur, based on applicable Privacy Laws.