

## EDWARDS VIEWFINDER SUBSCRIPTION AGREEMENT

This Edwards Viewfinder Subscription Agreement (“Agreement”) is entered into by and between Edwards Lifesciences LLC (“**Edwards**”) and a customer who issues a purchase order pursuant to an applicable quote (“**Customer**”) for the Services (as further defined below). Customer desires to buy the Services from Edwards at the prices set forth in the applicable quote. Edwards and Customer may be referred to in this Agreement individually as a “**Party**” and collectively as the “**Parties**”.

### BACKGROUND

Edwards manufactures and sells advanced hemodynamic monitoring platforms. It has developed and offers the Viewfinder suite of hemodynamic monitoring, statistical, analytical, and related web-based solutions on a software-as-a-service basis (as further defined below, the “Services”) for use within critical care settings of hospitals.

This Agreement, including the incorporated end user license agreement (“EULA”), sets out the terms and conditions that govern Customer’s access to and use of the Services during the Term of this Agreement pursuant to a Service Order issued under this Agreement.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained in this Agreement, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

#### 1. Definitions.

“**Access**” or “**Access to the Services**” shall mean access to and use of the Services (defined below), in each case pursuant to the terms and conditions of this Agreement.

“**Data Aggregation Services**” where included in the scope of Services as set forth in a Service Order, Data Aggregation Services means Edwards pooling data from multiple sources or customers in order to conduct analytics and provide data services relevant for the Customer, including the Customer’s use of the Services, and including, for example, benchmarking data, service utilization, and trend analysis.

“**Authorized User(s)**” means unique, identifiable employees or agents of Customer who Customer authorizes to have Access to the Service.

“**Business Associate Agreement**” or “**BAA**” means the business associate agreement by and between Edwards and Customer attached in Exhibit B, if applicable.

“**Credentials**” means any user name, identification number, password, license or security key, security token, PIN, or other security code, method, technology, or device, used alone or in combination, to verify an individual's identity and authorization to access and use the Services.

“**Customer Data**” means Raw Data (i) entered or uploaded into the Service by Customer, (ii) captured by the Service, and/or (iii) stored in and retrievable through the Service.

“**Databases**” means any and all databases in which all or any portion of the Service Data is stored.

“**De-Identified Data**” means de-identified or anonymized data as defined under applicable law or data that has been rendered to no longer be Personal Data in accordance with applicable laws. With respect to PHI, “De-Identified Data” means PHI that has been de-identified pursuant to 45 CFR § 164.514.

“**Edwards Intellectual Property**” means (i) the Service, including, without limitation, all software, software platforms, interfaces, code, and algorithms thereof; (ii) all Databases; (iii) all De-Identified Data (iv) all Edwards

Materials; (v) all Confidential Information of Edwards, (vi) Edwards' name, trademarks, service marks and logo(s), together with all goodwill associated therewith and (vii) any and all non-Customer data supplied to Edwards by its third party licensors or otherwise acquired by Edwards.

**“Edwards Materials”** means the Software, Services, documentation, De-Identified Data, all resulting data and analytics from Data Aggregation Services, and any and all other information, data, documents, materials, works, and other content, devices, methods, processes, hardware, software, and other technologies and inventions, including any deliverables, technical or functional descriptions, requirements, plans, or reports, that are provided or used by Edwards in connection with the Services or otherwise comprise or relate to the Services or Edwards computer systems. For the avoidance of doubt, Edwards Materials include De-Identified Data and any information, data, or other content derived from Edwards's provision and monitoring of Customer's access to or use of the Services, but do not include Customer Data.

**“EULA”** means the end user license agreement terms presented to users, which is available at ([http://edwards.com/ViewfinderRemote\\_EULA](http://edwards.com/ViewfinderRemote_EULA)) and incorporated herein by reference, as they may be updated from time to time.

**“Harmful Code”** means any software, hardware, or other technology, device, or means, including any virus, worm, malware, or other malicious computer code, the purpose or effect of which is to (a) permit unauthorized access to, or to destroy, disrupt, disable, distort, or otherwise harm or impede in any manner any (i) computer, software, firmware, hardware, system, or network; or (ii) any application or function of any of the foregoing or the security, integrity, confidentiality, or use of any data Processed thereby; or (b) prevent Customer or any Authorized User from accessing or using the Services or Edwards Systems as intended by this Agreement. Harmful Code does not include any Edwards Disabling Device.

**“Intellectual Property”** or **“Intellectual Property Right(s)”** means any patent, copyright, trademark, service mark, trade secret, or other intellectual property of any nature or kind belonging to, or controlled by, a Party, whether protected, created, or arising under any United States federal, state or local law, or under any federal, state or local law of any other country, or under any international treaty or convention, and all right, title and interest therein and thereto

**“Patient”** means an individual Person with respect to whom Customer possesses Raw Data.

**“Person”** means any individual, corporation, partnership, limited liability company, joint venture, trust, unincorporated organization, government or any agency or instrumentality thereof, or other juridical person recognized by law.

**“Personal Data”** means information relating to an identified or identifiable person, including “PHI” and “ePHI”. “PHI” and “ePHI” are defined under the BAA on Exhibit B.

**“Process”** means to take any action or perform any operation or set of operations that the Services are capable of taking or performing on any data, information, or other content, including without limitation to collect, receive, input, upload, download, record, reproduce, store, organize, compile, combine, aggregate, log, catalog, cross-reference, manage, host, maintain, copy, adapt, alter, translate, modify, manipulate, reformat, or make other derivative works or improvements, analyze, process, retrieve, output, consult, use, perform, display, disseminate, transmit, submit, post, transfer, disclose, or otherwise provide or make available, or block, erase, or destroy. “Processing” and “Processed” have correlative meanings.

**“Raw Data”** means all data (including all Personal Data) related to a Patient created, collected and/or maintained by or on behalf of Customer, as such data exists immediately before it is entered or uploaded into the Service by Customer.

**“Services”** means Edwards' provision of access to the Software on a software-as-a-service basis, as more particularly described in the respective Service Orders entered into hereunder.

“**Service Data**” means Customer Data and De-Identified Data.

“**Service Order**” means the document, substantially in the form attached hereto as **Exhibit A** (**Exhibit A** means **Exhibit A-1**, and any subsequently numbered **Exhibit A** if applicable (i.e., A-2, A-3, etc.), identifying a Service to be provided by Edwards to Customer hereunder, together with the Fees payable in connection therewith, the number of Authorized Users to be provided Access and certain other information.

“**Software**” means the Viewfinder suite of hemodynamic monitoring, statistical, analytical, and related software solutions, as they are made available and updated from time to time by Edwards in its discretion, as more specifically identified in one or more Service Orders.

“**Subscription Term**” means the period during which authorized users may have Access to the Services as set forth in the applicable the Service Order Form.

## 2. Services.

a. Access and use. Subject to and conditioned upon Customer’s and its Authorized Users’ compliance with the terms and conditions of this Agreement, including the EULA, Edwards grants to provide Customer a non-exclusive, non-transferrable (except in compliance with Section 21), non-sublicensable license to access and use the Services in the United States during the Term, solely for Customer’s internal use (which includes, without limitation, patient care) by its Authorized Users in accordance with (i) this Agreement, (ii) the Business Associate Agreement, and (iii) each Service Order issued under this Agreement. The total number of Authorized Users may not exceed the number set forth in the applicable Service Order(s), except as expressly agreed to in writing by the parties and subject to any appropriate adjustment of the Fees payable under this Agreement and the applicable Service Orders.

b. Service levels. Subject to the terms and conditions of this Agreement, Edwards will use commercially reasonable efforts to provide the Services in accordance with the terms of the Service Level Agreement attached as Exhibit C.

c. Documentation. Edwards hereby grants to Customer a non-exclusive, non-sublicensable, non-transferrable (except in compliance with Section 21) license to use the Services-related documentation during the Term solely for Customer’s internal business purposes in connection with its use of the Services.

d. Changes. Edwards reserves the right, in its sole discretion, to make any changes to the Software, the Services, the EULA, and the Edwards Materials that it deems necessary or useful to: (a) maintain or enhance: (i) the quality or delivery of Edwards’ services to its customers; (ii) the competitive strength of or market for Edwards’ services; (iii) the Services cost efficiency, performance, or security; or (b) to comply with applicable federal, state, or local laws, regulations, or rules.

e. Reservation of rights. Subject to the license grants set forth in this Section 2 and the EULA, and except as otherwise set forth in this Agreement: (i) Edwards exclusively owns and reserves all right, title and interest in and to the Services, including without limitation all Edwards Intellectual Property Rights and Edwards Materials therein; and, (ii) no other license, right, title, or interest in and to the Services (or any Edwards Intellectual Property Right or Edwards Materials therein) is granted, whether explicitly or implicitly, to Customer under this Agreement or any Service Order.

3. Restrictions on Use; Customer Responsibilities.

a. Customer shall not, and shall not permit any other Person to, access or use the Services, Software, or Edwards Materials except as expressly permitted by this Agreement and in accordance with the EULA.

b. Without limiting the generality of Section 2, Customer shall not, except as this Agreement expressly permits:

i. copy, modify, or create derivative works or improvements of the Software, Services, or Edwards Materials;

ii. rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available any Services or Edwards Materials to any Person, including on or in connection with the internet or any time-sharing, service bureau, software as a service, cloud, or other technology or service;

iii. reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Software, Services, or Edwards Materials, in whole or in part;

iv. bypass or breach any security device or protection used by the Services or Edwards Materials; or access or use the Software, Services, or Edwards Materials other than by an Authorized User through the use of his or her own then valid Credentials; or attempt to do any of the foregoing;

v. input, upload, transmit, or otherwise provide to or through the Services or Edwards Systems, any information or materials that are unlawful or injurious, or contain, transmit, or activate any Harmful Code;

vi. damage, destroy, disrupt, disable, impair, interfere with, or otherwise impede or harm in any manner the Services, Edwards Systems, or Edwards's provision of services to any third party, in whole or in part;

vii. remove, delete, alter, or obscure any trademarks, specifications, documentation, End User License Agreement, warranties, or disclaimers, or any copyright, trademark, patent, or other intellectual property or proprietary rights notices from the Software, any Services, or any Edwards Materials, including any copy thereof;

viii. access or use the Software, Services, or Edwards Materials in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Right, privacy right, or other right of any third party, or that violates any applicable law;

ix. access or use the Services or Edwards Materials for purposes of competitive analysis of the Services or Edwards Materials, the development, provision, or use of a competing software, service, or product;

x. otherwise access or use the Services or Edwards Materials beyond the scope of the authorization granted under this Section 2.

c. Customer shall:

i. be solely responsible for controlling each Authorized User's access to Services; without limiting the breadth of the foregoing, Customer shall be responsible for assigning and revoking permissions to Authorized Users, for periodically verifying Authorized Users' permission to access the Services, for maintaining the security of single-sign-on systems used to access the Services, and for implementing multifactor authentication and other security measures in accordance with law and industry best practices;

ii. be responsible for each Authorized User's compliance with the terms and conditions of this Agreement and the EULA, and be liable for the breach by any such Authorized User of the terms and conditions of this Agreement;

iii. determine the need for, and if necessary, be responsible for securing, written consents and/or authorizations from Patients as may be required per Customer's internal policies and procedures or as otherwise required by applicable laws in order to permit (A) Customer to enter or upload Raw Data into the Service, (B) Edwards to access, subject to the limitations described in this Agreement, Process such Raw Data (including, without limitation, by and through any and all of Edwards' third-party service providers), and (C) Edwards to provide the Services to Customer, in each case in the manner contemplated herein, without violating the privacy or other rights of any Patient or other Person;

iv. be responsible for the accuracy, quality and legality of all Raw Data, and the means by which Customer acquires all Raw Data;

v. use commercially reasonable efforts to prevent unauthorized access to or use of Services, including commercially reasonable precautions to ensure that each Credential is maintained as Confidential Information, and notify Edwards promptly of any unauthorized access to or use of the Services of which Customer becomes aware; and

vi. use the Services only as permitted by and in accordance with this Agreement and the EULA, and all applicable federal, state and local laws, rules and regulations.

#### **4. Customer Data; Feedback.**

a. Ownership. As between Edwards and Customer, Customer shall own all right, title, and interest in and to Customer Data. Edwards acquires only the limited rights and licenses expressly granted by this Agreement.

b. Use of Customer Data. Subject to the terms and conditions of this Agreement, Customer hereby grants to Edwards a non-exclusive, perpetual, royalty-free license to Process Raw Data and Customer Data as necessary or useful for (a) Edwards' provision of the Services to Customer under this Agreement, including training, demonstration, research, development, benchmarking, continuous improvement, and facilitating the provision of its products, software and services, (b) Edwards' creation and use of De-Identified Data, and (c) Edwards' maintenance and development of current and future Services.

c. Feedback. Customer grants to Edwards a non-exclusive, royalty-free license to use, share, and commercialize, in any way and for any purpose, and without charge or other compensation, any suggestion, enhancement request, recommendation, correction or other feedback relating to the Services that Customer provides to Edwards (collectively, "**Feedback**"). Customer acknowledges and agrees that all right, title and interest in and to any modifications to, or new versions or releases of the Services arising from Edwards' use, incorporation and/or implementation of Feedback, including without limitation, all Edwards Intellectual Property Rights therein, are and shall be owned exclusively by Edwards, and that no right, title, or interest in the Services or any portion thereof, or any modifications thereto, new versions or releases thereof, shall be granted to Customer hereunder, except as may be included in the license grant set forth in Section 2 hereof.

d. Customer Reservation of Rights. Subject to the licenses granted in Section 2 and except as otherwise set forth in this Agreement: (i) Customer reserves all right, title and interest in and to the Raw Data, Customer Data, Customer's Intellectual Property, and Customer Confidential Information, (ii) no other right, title, or interest in and to the Raw Data, Customer Data, Customer's Intellectual Property and Customer Confidential Information is granted to Edwards hereunder.

## 5. Confidentiality.

a. Confidential Information. The term “**Confidential Information**” shall mean all confidential and/or proprietary documents and information that a disclosing Party or representatives (collectively, “**Disclosing Party**”) has provided or will provide or otherwise has made or will make accessible to a receiving Party or representatives (collectively, “**Receiving Party**”), pursuant to or in contemplation of this Agreement, in each case whether provided or made accessible at any time prior to or subsequent to the Effective Date of this Agreement, and whether tangible or intangible, and in whatever form or medium (e.g., written, oral, graphic, electronic or other form), including without limitation the terms and conditions of this Agreement and any service orders issued hereunder (including all Fees set forth therein), all Intellectual Property, business operations, marketing plans, patient information, customer lists, financial data, and any other documents and information pertaining to the business of the Disclosing Party, as well as all documents and information generated by the Receiving Party that contain, reflect, or are derived from the documents and information provided or made accessible by the Disclosing Party to the Receiving Party. Notwithstanding the foregoing, “Confidential Information” shall not include any information: (i) that, at the time of disclosure, is or was generally available to the public; (ii) that, after disclosure hereunder, becomes generally available to the public, except as a result of a breach of this Agreement by the Receiving Party; (iii) that becomes available to the Receiving Party from a third party that is not legally or contractually prohibited by the Disclosing Party from disclosing such Confidential Information; or, (iv) that the Receiving Party can demonstrate was developed by or for the Receiving Party without access to or use of the Confidential Information. For the avoidance of doubt, (x) the Edwards Intellectual Property shall be deemed Confidential Information of Edwards, and shall be and remain subject to the terms and conditions of this Agreement, and (y) the Raw Data and Customer Data shall be deemed Confidential Information of Customer, and shall be and remain subject to the terms and conditions of this Agreement.

b. **Duty of Nondisclosure.** The parties agree (a) to hold the other’s Confidential Information in confidence, using the same degree (but no less than a reasonable degree) of care and protection that it exercises with its own confidential information of a similar nature; (b) not to directly or indirectly disclose, copy, distribute, republish or allow access to any Confidential Information of the other party to a third party; and (c) not to use the other party’s Confidential Information for any purpose other than as necessary to fulfill such party’s obligations or exercise its rights under this Agreement. Notwithstanding the above, either Party may disclose Confidential Information to the extent that it is required by law or regulation (including court order or subpoena or other governmental decree or authority), provided that the Receiving Party, if required by governmental authority to reveal Confidential Information of the Disclosing Party shall, if allowed by law, notify the disclosing party promptly upon learning of the government requirements and before making such disclosure, and shall provide the Disclosing Party with an opportunity (at the disclosing party’s own expense) to seek a protective order or other appropriate procedure so that the disclosure, if required, can be made in a manner than preserves the confidentiality of the Confidential Information.

**6. Intellectual Property and Assets.** Customer acknowledges and agrees that Edwards is and shall remain the owner of all right, title and interest in and to the Edwards Intellectual Property. Except as otherwise set forth in this Agreement: (i) Customer shall have no right, title or interest in or to any Edwards Intellectual Property or any portion(s) thereof; (ii) nothing in this Agreement shall operate or be construed as an express or implied grant, transfer, conveyance, assignment or license to the Customer of any right, title or interest in and to any Edwards Intellectual Property; and, (iii) upon expiration or termination of this Agreement, Customer shall immediately cease any and all further use and disclosure of the Edwards Intellectual Property unless and until a superseding agreement is executed between the Parties. Customer shall take such actions (including, without limitation, execution of affidavits or other documents) as Edwards may reasonably request, to effect, perfect, or confirm Edwards’ ownership interests and other rights as set forth in this Section 6.

## 7. Fees and Payment.

a. **Fees.** Customer shall pay to Edwards fees for Services (collectively, “**Fees**”) in the amounts set forth in each Service Order issued under this Agreement.

b. **Invoicing and Payment.** Customer's issuance of a purchase order is not a condition precedent to Customer's obligation to pay the Fees to Edwards. If Customer's policies require the issuance of a purchase order, Customer shall issue purchase orders for the Services and the applicable Fees concurrently with the execution of this Agreement and any Service Order(s), and at least ninety (90) days prior to the renewal of the Service Order, if applicable. Edwards shall invoice Customer in advance in accordance with each Service Order. Unless otherwise provided in a Service Order, invoiced charges shall be due net thirty (30) days from the invoice date. If any issuance of a purchase order or amount due and owing by Customer hereunder (including pursuant to any Service Order) is thirty (30) or more days overdue, Edwards may, without limiting its other rights and remedies, suspend any portion or all Services provided to Customer hereunder or under any Service Orders until such amounts are paid in full. Edwards shall give Customer at least ten (10) days' prior notice that its account is overdue before so suspending any Services.

c. **Overdue Fees.** In the event that any invoiced amount is not received by Edwards when due, then without limiting Edwards' rights or remedies: (i) such amounts shall accrue interest at the rate of 1.5% of the outstanding balance per month or, if lower, the maximum rate permitted by law; and (ii) Edwards may condition all subsequent subscription renewals and Service Orders on payment terms shorter than those specified in Section 6(b).

d. **Taxes.** Fees do not include any taxes, levies, duties or similar governmental assessments of any nature, including, for example, value-added, sales, use or withholding taxes, assessable by any jurisdiction whatsoever (collectively, "**Taxes**"). Customer shall be and remain responsible for paying all Taxes associated with Customer's subscription for and use of the Services hereunder.

**8. Compliance with Laws; No Obligation to Purchase.** Each Party agrees to comply with the provisions of the Business Associate Agreement set forth in Exhibit B that is hereby incorporated into this Agreement, with respect to such Party's use and disclosure of PHI. Each party also agrees to comply with all applicable federal, state and local laws and regulations of the jurisdiction wherein it conducts business. It is the express understanding of the Parties that none of the rights or obligations set forth in this Agreement are contingent or predicated upon Customer's purchase of any products or services from Edwards, and that this Agreement is not entered into with the intent to induce or in exchange for any explicit or implicit agreement or understanding that Edwards' products or services will be purchased, leased, ordered, prescribed or recommended by or to Customer.

**9. Disclaimer of Warranties.**

BECAUSE THE SERVICES INVOLVE THE PROCESSING OF RAW DATA ENTERED OR UPLOADED INTO THE SERVICE BY PERSONS OTHER THAN EDWARDS, EDWARDS DOES NOT AND CANNOT ENSURE, REPRESENT, WARRANT OR GUARANTEE THE ACCURACY, COMPLETENESS OR RELIABILITY OF THE SERVICES OR THE DATA CONTAINED IN THE VARIOUS EDWARDS DATABASES UPON WHICH THE SERVICES ARE DEPENDENT. CUSTOMER IS SOLELY RESPONSIBLE FOR THE RAW DATA ENTERED OR UPLOADED INTO THE SERVICE BY CUSTOMER'S AUTHORIZED USERS.

THE SERVICES ARE NOT INTENDED TO BE USED AS A BASIS FOR ANY DECISION (INCLUDING WITHOUT LIMITATION ANY DECISION REGARDING THE DIAGNOSIS, CURE, TREATMENT, MITIGATION OR PREVENTION OF ANY DISEASE, ILLNESS OR OTHER MEDICAL CONDITION OR IMPAIRMENT), OR TO SERVE AS A SUBSTITUTE FOR PROFESSIONAL MEDICAL ADVICE.

EXCEPT AS EXPRESSLY PROVIDED HEREIN AND IN THE BUSINESS ASSOCIATE AGREEMENT, THE SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. EDWARDS MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICES (INCLUDING WITHOUT LIMITATION THE MATERIALS) AND ANY OTHER EDWARDS ASSETS SUPPLIED OR OTHERWISE MADE AVAILABLE TO CLIENT BY EDWARDS HEREUNDER, AND EDWARDS HEREBY EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES WITH RESPECT THERETO, INCLUDING WITHOUT LIMITATION, ANY WARRANTIES AS TO THE

RELIABILITY, ACCURACY, COMPLETENESS OR TIMELINESS OF THE SERVICES (AND THE MATERIALS) OR ANY OTHER EDWARDS ASSETS, ANY EXPRESS OR IMPLIED WARRANTIES OF QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, OR NON-INFRINGEMENT (INCLUDING, WITHOUT LIMITATION, NON-INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT, PRIVACY RIGHT, OR OTHERWISE), OR ANY WARRANTIES ARISING FROM A COURSE OF DEALING OR TRADE PRACTICE. EDWARDS SPECIFICALLY DOES NOT WARRANT THAT THE SITE OR THE SERVICES WILL OPERATE WITHOUT ERROR OR INTERRUPTION OR THAT ALL ERRORS AFFECTING THE SITE OR THE SERVICES, SHOULD THEY ARISE, WILL BE CORRECTED.

**10. Limitation of Liability.** EXCEPT FOR (A) THE PARTIES' RESPECTIVE INDEMNIFICATION OBLIGATIONS UNDER SECTION 12, (B) THE PARTIES' CONFIDENTIALITY OBLIGATIONS UNDER SECTION 5, (C) THE PARTIES' OBLIGATIONS UNDER THE SEPARATE BAA, AND (D) CUSTOMER'S OBLIGATION TO PAY THE FEES, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY AMOUNT IN EXCESS THE AMOUNT PAID UNDER THIS AGREEMENT DURING THE SIX MONTH PERIOD PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

**11.** EXCEPT WITH RESPECT TO LIABILITY ARISING UNDER THE PARTIES' RESPECTIVE INDEMNIFICATION OBLIGATIONS UNDER SECTION 12, CONFIDENTIALITY OBLIGATIONS UNDER SECTION 5, AND OBLIGATIONS UNDER THE SEPARATE BAA, UNDER NO CIRCUMSTANCES SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY TYPE OF INCIDENTAL, SPECIAL, PUNITIVE, INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST REVENUE, LOST PROFITS, LOSS OF TECHNOLOGY, RIGHTS OR SERVICES, LOSS OF INFORMATION, OR INTERRUPTION OR LOSS OF USE OF SERVICE OR EQUIPMENT, ARISING OUT OF OR IN ANY MANNER CONNECTED WITH OR RELATING TO THIS AGREEMENT OR THE SUBJECT MATTER HEREOF, WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED, REGARDLESS OF THE FORM OF ACTION, AND REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING, WITHOUT LIMITATION, WHETHER ARISING UNDER ANY THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE), EVEN IF A PARTY HAS BEEN INFORMED OF, OR OTHERWISE MIGHT HAVE ANTICIPATED, THE POSSIBILITY OF SUCH DAMAGES. THE PARTIES ACKNOWLEDGE THAT THE PARTIES HAVE ENTERED INTO THIS AGREEMENT IN RELIANCE UPON THE LIMITATIONS OF LIABILITY AND THE DISCLAIMERS OF WARRANTIES AND DAMAGES SET FORTH IN THIS AGREEMENT, AND THAT THE SAME FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES. THE PARTIES AGREE THAT THE LIMITATION AND EXCLUSIONS OF LIABILITY AND DISCLAIMERS SPECIFIED IN THIS AGREEMENT WILL SURVIVE AND APPLY EVEN IF FOUND TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

**12. Indemnification; Insurance.**

a. Indemnification by Edwards. Edwards shall defend, indemnify and hold harmless Customer its officers, directors, agents and employees, against all claims, liabilities, damages, losses and expenses, including reasonable attorneys' fees and cost of suit (except as otherwise provided in Section (c) below) ("**Losses**"), to the extent arising out of any claim, demand, suit or proceeding made or brought against Customer by a third Person arising out of or based upon (i) an allegation of the gross negligence, grossly negligent omissions or willful misconduct of Edwards or any of Edwards' employees, agents or subcontractors, or (ii) an allegation against Customer that the Software or Services provided under this Agreement infringe the Intellectual Property Rights of a third Person.

b. Indemnification by Customer. Customer shall defend, indemnify and hold harmless Edwards its officers, directors, agents and employees, against all Losses, to the extent arising out of any claim, demand, suit or proceeding made or brought against Edwards by a third Person arising out of or based upon (i) an allegation that Customer's use of any Raw Data, Service Data, and/or any Edwards Intellectual Property in combination with

any assets, materials or other things not provided or authorized by Edwards, infringes or misappropriates such third Person's Intellectual Property Rights; (ii) an allegation that the Raw Data violates a third Person's privacy rights or other rights; (iii) a non-Edwards application, product or service; (iv) an allegation of the gross negligence, grossly negligent omissions or willful misconduct of Customer or any of Customer's employees, agents or subcontractors.

c. Indemnification Procedures. The Party entitled to make a claim for indemnification under this Section 12 shall be referred to as the "**Indemnified Party**" and the Party required to indemnify such claim shall be referred to as the "**Indemnifying Party**." In order for an Indemnified Party to be entitled to any indemnification provided for under this Agreement in respect of, arising out of or involving a claim or demand, made by any third Person against the Indemnified Party (a "**Third Party Claim**"), such Indemnified Party must promptly notify the Indemnifying Party in writing of the Third Party Claim after receipt by such Indemnified Party of written notice of the Third Party Claim; *provided, however*, that failure to give such notification shall not affect the indemnification provided hereunder except to the extent the Indemnifying Party shall have been actually materially prejudiced as a result of such failure. If a Third Party Claim is made against an Indemnified Party, the Indemnifying Party shall assume the defense thereof and the Indemnified Party shall have the right (but not the duty) to participate in the defense thereof and to employ counsel, at its own expense, separate from the counsel employed by the Indemnifying Party. The Indemnifying Party shall be liable for the fees and expenses of counsel employed by the Indemnified Party for any period during which the Indemnifying Party has not assumed the defense thereof, but the Indemnifying Party shall not be liable to the Indemnified Party for any legal expenses subsequently incurred by the Indemnified Party in connection with the defense thereof. The Parties hereto shall cooperate in the defense or prosecution thereof of any Third Party Claim. Such cooperation shall include the retention and (upon the Indemnifying Party's reasonable request) the provision to the Indemnifying Party of records and information which are reasonably relevant to such Third Party Claim at the Indemnifying Party's expense, and making employees or any other Indemnified Party available on a mutually convenient basis to provide additional information and explanation of any material provided hereunder. The Indemnifying Party shall not admit any liability with respect to, or settle, compromise or discharge, such Third Party Claim without the Indemnified Party's prior written consent, which shall not be unreasonably withheld.

d. **Insurance.** Each Party shall procure and maintain in effect (i) commercial general liability insurance covering its acts and omissions, and those of its agents and employees, in the amounts of not less than One Million Dollars (\$1,000,000) per occurrence and Three Million Dollars (\$3,000,000) in aggregate; and (ii) Information Security and Privacy Insurance in an amount not less than Five Million Dollars (\$5,000,000). Each Party may elect to satisfy this requirement by electing to self-insure all or a portion of these limits.

The Parties acknowledge that the minimum amounts and types of insurance coverage required in this paragraph shall not be construed to create a limit to each Party's liability with respect to its indemnification obligations in this Agreement.

### **13. Term and Termination.**

a. Term of Agreement. The term of this Agreement shall begin on the Effective Date and shall continue in full force and effect until the date of expiration or termination of all Service Orders issued hereunder, unless terminated earlier in accordance with this Agreement (the "**Term**").

b. Subscription Term. The Subscription Term for each Service subscribed for under this Agreement shall be as specified in the applicable Service Order.

c. Termination. Either Party may terminate this Agreement for cause: (i) if the other Party breaches any term or condition of this Agreement which remains uncured as of the date thirty (30) days after notice thereof from the non-breaching Party (*provided, however*, that if the breach involves the failure to pay Fees in accordance with the terms or conditions of this Agreement, Customer shall have ten (10) days to cure such breach following receipt of notice thereof from Edwards); or (ii) if the other Party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

In the event that this Agreement is terminated in accordance with this Section as a result of such a breach, the non-breaching Party shall, in addition to its rights of termination, be entitled to pursue all other remedies against the breaching party, whether at law or in equity.

d. Suspension of Services for System Integrity. In addition to Edwards' rights of termination under Section 13(c), Edwards shall have the right to suspend Customer's Access to the Services, in whole or in part and without notice to Customer: (i) if Edwards reasonably believes that Customer's or its Authorized User's Access to the Services represents a direct or indirect threat to the function or integrity of the Services, Edwards' or its service provider's networks or Intellectual Property, or any other Person's access to and use of the Services; (ii) if reasonably necessary to prevent unauthorized access to any Raw Data, Service Data, Databases, and/or Confidential Information; and/or (iii) to the extent necessary to comply with any applicable federal, state and local laws, rules and regulations. If Edwards suspends Customer's Access to the Services without notice, Edwards will provide the reason for such suspension to Customer. Any suspension of Customer's Access to the Services for the foregoing reasons will be in effect for as long as reasonably necessary to address the issues giving rise to the suspension.

e. Effect of Termination or Expiration. Upon any expiration or termination of this Agreement, except as expressly otherwise provided in this Agreement:

i. all licenses granted to Customer under this Agreement shall immediately terminate;

ii. Edwards may disable all Customer and Authorized User Access to the Software, Services, and Edwards Materials;

iii. all Fees that would have become payable had the Agreement remained in effect until expiration of the Term will become immediately due and payable, and Customer shall pay such Fees, together with all previously accrued but not yet paid Fees, upon receipt of Edwards's invoice therefor; and

iv. if Customer requests in writing within at least thirty (30) days following the effective date of expiration or termination, Edwards shall, within ninety (90) days following such expiration or termination, deliver to Customer the then most recent version of Customer Data maintained by Edwards, provided that Customer has at that time paid all Fees then outstanding and any amounts payable after or as a result of such expiration or termination, including any reasonable expenses and fees for Edwards' services in transferring such Customer Data.

f. Survival. The following provisions of this Agreement shall survive expiration or any earlier termination of this Agreement for any reason: Sections 1, 2(c)(e), 3-7, 8-12, 13(e), 14, 17-25.

#### **14. Data Security.**

e. Data Backup. The Services do not replace the need for Customer to maintain regular data backups or redundant data archives. EDWARDS HAS NO OBLIGATION OR LIABILITY FOR ANY LOSS, ALTERATION, DESTRUCTION, DAMAGE, CORRUPTION, OR RECOVERY OF CUSTOMER DATA.

f. Data Security. Edwards will employ information security measures in accordance with its Data Security Policy, as amended from time to time, a current copy of which is attached as Exhibit D.

g. Access and Security. Customer shall employ all physical, administrative, and technical controls, screening, and security procedures and other safeguards necessary to: (a) securely administer the distribution and use of all Credentials and protect against any unauthorized access to or use of the Services; and (b) control the content and use of Customer Data, including the uploading or other provision of Customer Data for Processing by the Services.

15. **Publications.** Customer may publish, present, or publicly disclose its clinical results in connection with this Agreement only upon providing Edwards the opportunity to review such results prior to Customer publishing or publicly disclosing such results. Customer agrees that Edwards may (i) use, refer to, and disseminate reprints of such publications; (ii) use Customer's name in its own case studies, testimonials, announcements, news releases, statements, or other publications relating to this Agreement for advertising, promotional or other purposes; and (iii) publish analyses of Aggregated or De-identified data.
16. **Force Majeure.** Neither Party shall be responsible for any delay or failure in performance under this Agreement or any Service Order if such delay or failure is caused by or attributable to flood, riot, insurrection, fire, earthquake, explosion, act of God, lack or failure of transportation facilities or services, internet service Edwards failure or delay, communication line failure, power line failure, or any other force or cause beyond the reasonable control of the Party claiming the protection of this Section 16. If any of the above enumerated circumstances prevent, hinder or delay performance of either Party's obligations under this Agreement or any Service Order for more than thirty (30) calendar days, the Party not prevented from performing may choose, at its option, to immediately terminate this Agreement without liability or penalty as of the date specified by such Party in a written notice of termination to the other Party. The Parties acknowledge and agree that labor shortages, disputes and strikes shall not be considered a force majeure event hereunder.
17. **Notices.** Any notices permitted or required hereunder shall be deemed effective if made in writing and sent by hand delivery, by facsimile, by certified mail (postage prepaid) return receipt requested, or by internationally recognized courier requiring a signature acknowledging receipt, to the following addresses, or to such other addresses as either Party may designate by notice issued hereunder (which such notices shall be effective when received):

Edwards: Edwards Lifesciences LLC  
 One Edwards Way  
 Irvine, CA 92614  
 Attention: Lance Maish, Healthcare Solutions – Commercial Contracts

With a copy to: Edwards Lifesciences LLC  
 One Edwards Way  
 Irvine, CA 92614  
 Attention: Law Department

Customer: Address identified in the  
 applicable Quote for Services  
 Attn: Contracts

With a copy (which shall not be deemed notice) to:  
 Address identified in the  
 applicable Quote for Services  
 Attn: Legal Department

18. **Entire Agreement.** This Agreement (and the Service Order Forms, Exhibits and/or Schedules hereto), together with the Business Associate Agreement, sets forth the entire agreement between the Parties with respect to the subject matter hereof, and supersedes all prior and contemporaneous agreements, arrangements or understandings, whether written or oral, concerning the subject matter hereof. No

modification of or amendment to this Agreement will be effective unless made in writing and signed by the Parties hereto.

19. **Conflicts.** In the event of a conflict between the provisions of this Agreement and any Service Order Form, hospital invoice or hospital purchase order, the provisions of this Agreement shall govern. In the event of any inconsistency or conflict between this Agreement and the Business Associate Agreement, the terms, provisions and conditions of the Business Associate Agreement shall govern and control.
20. **Severability.** If the application of any provision of this Agreement and/or any Service Order to any particular facts or circumstances shall be held to be invalid or unenforceable by a court of competent jurisdiction, then: (a) the validity and enforceability of such provision as applied to any other particular facts or circumstances, and the validity and enforceability of the other provisions of this Agreement and/or any Service Order (as applicable), shall not in any way be affected or impaired thereby and (b) such provision shall be enforced to the maximum extent possible so as to effect the intent of the Parties and shall be reformed without further action by the Parties to the extent necessary to make such provision valid and enforceable while preserving the original intent of the Parties.
21. **Assignment.** Neither this Agreement nor any Service Order, including without limitation, any of the rights, duties and obligations hereunder or thereunder, can be delegated or assigned, in whole or in part, by either Party without the prior written consent of the other Party, provided that Edwards may assign this agreement to any successor of all or substantially all of the business to which this Agreement relates without the prior consent of Customer.
22. **Waiver.** No express or implied waiver by a Party of any breach or default of any term or condition of this Agreement or any Service Order will be construed as a waiver of a future or subsequent breach or default. The failure or delay of any Party in exercising any of its rights under this Agreement or any Service Order will not constitute a waiver of any such right, and any single or partial exercise of any particular right by any Party will not exhaust the same or constitute a waiver of any other right provided in this Agreement or any Service Order.
23. **Governing Law.** This Agreement and each Service Order shall in all respects be governed by, and construed and interpreted in accordance with, the laws of the State of California without giving effect to any conflicts of law principles of such state that might refer the governance, construction or interpretation of this Agreement to the laws of another jurisdiction.
24. **No Third Party Beneficiaries.** This Agreement and each Service Order are intended solely for the mutual benefit of the Parties hereto and there is no intention, expressed or otherwise, to create any rights or interests for any other entity(ies) or person(s) other than the Parties hereto.
25. **Independent Contractor.** The status of the Parties hereunder shall be that of independent contractors. Neither Party is or shall be deemed an employee, agent or representative of the other Party. Neither Party shall have any right, power, or authority to enter into any agreement for or on behalf of the other Party, or to incur any obligation or liability or otherwise bind the other Party. Neither this Agreement nor any Service Order shall create an association, joint venture, or partnership between the Parties nor impose any partnership liability upon either Party. Each Party shall be solely responsible for compensating and providing benefits to any person(s) providing services on its behalf and for ensuring that any associated taxes or other payments due are paid.
26. **Exclusion from Federal Healthcare Programs.** Each Party represents to the best of its knowledge that it is not debarred, suspended, excluded or otherwise ineligible to participate in any federal or state healthcare program. Should either Party become debarred, suspended,

excluded or otherwise ineligible to participate in any federal or state healthcare program, the other Party shall have the right to immediately terminate this Agreement.

27. **Exhibit List.** The exhibits included in this Agreement are set forth in the table below.

<b>EXHIBIT</b>	<b>TITLE</b>
A-1	Service Order Form
B	Business Associate Agreement
C	Service Level Agreement
D	Information Security Practices for the Viewfinder Network

## EXHIBIT A-1

### SERVICE ORDER FORM

This Service Order shall be effective upon Viewfinder Hub installation (“Service Effective Date”)

<b>Service Term:</b>	The number of years purchased in the applicable quote, following Viewfinder Hub installation on hospital virtual machine or server
----------------------	--

Services and Processing Fees	Service Fees	Total Monitors	Total Service Fee
1. Service Fee for Viewfinder	As set forth in applicable Quote	As set forth in applicable Quote	As set forth in applicable Quote

**Table 1. Services**

**Software Service (check applicable Services to be licensed by Customer under this Service Order Form):**

- Viewfinder**, includes the following:

**Viewfinder Hub:** Single pipeline for real-time bidirectional data interchange utilizing a wireless or connection. Enables secure connectivity between HemoSphere, hospital information systems, Edwards Cloud, other 3<sup>rd</sup> party devices. Deployed on hospital network via virtual installation.

**Viewfinder Remote:** A remote view application specific to viewing the data from associated Edwards’ technologies. Enables user to view data utilizing their mobile device inside and outside of the facility.

**Viewfinder Devices:** A device management and security web application that includes remote monitoring of system health and machine diagnostics and proactive maintenance alerts.

The following steps are required to setup and enable the Viewfinder solution:

**Pre-install process to prepare for go-live:**

- Edwards team to align with Customer to determine the resource team
- Team resources, users identified and matched to go live process
- Alignment with IT on prioritization and process to install software
- Scope of install, go-live process communicated to team

**Setup Viewfinder Hub on a virtual machine:**

- Customer to identify/create a virtual machine or server
- Customer to provide Edwards access to virtual machine or server
- Edwards to download and install on virtual machine or server

**Resource Training:**

- Edwards to provide training prior to go live of Viewfinder Network application(s) and support Customer identification of its identifiers, users, and roles of each application (any additional training may be subject to additional support fees)
- Edwards to work with Customer to setup accounts for users
- Edwards to train users on software application(s)
- Users to setup desired account preferences

**Ongoing support of Viewfinder Network application(s):**

- Edwards to provide technical service and support through term of agreement
- Additional reconfiguring fees may apply if hospital requests changes from the original mapping to the virtual machine or server

**Setup EMR Data Extract and sFTP:**

- Customer to identify targeted service line or procedure group (e.g., operating room, critical care unit)
- Customer to identify EMR system analyst for data query, validation and daily extract
- Customer to identify IT analyst to configure and schedule data refresh and transfer via sFTP

Following the initial purchase order for Service, Customer shall issue to Edwards a purchase order for subscription fees at least ninety (90) days prior to the renewal .

## EXHIBIT B

### BUSINESS ASSOCIATE AGREEMENT

**THIS BUSINESS ASSOCIATE AGREEMENT** (“Agreement” or “BAA”) is made a part of and fully incorporated into the Edwards Viewfinder Subscription Agreement and/or an applicable statement of work or other written agreement consistent with this BAA (“Underlying Agreement”) entered into by and between Customer who issues a purchase order for the Services in the Underlying Agreement (“Covered Entity”) and Edwards Lifesciences LLC (“Edwards”) (collectively, the “Parties”).

#### **RECITALS:**

**WHEREAS**, Edwards and Covered Entity have entered into the Underlying Agreement that involves the provision of Services (defined below) by Edwards to Covered Entity and may involve the use and/or disclosure of Protected Health Information (defined below); and

**WHEREAS**, the Parties desire to enter into this Agreement in order to comply with the provisions of HIPAA (defined below);

**NOW, THEREFORE**, in consideration of the mutual promises and undertakings herein contained, the Parties agree as follows:

1. **Terms.** Capitalized terms used but not otherwise defined in this BAA shall have the same meaning as those terms in 45 CFR Parts 160 and 164.

**Business Associate.** “Business Associate” shall mean Edwards Lifesciences LLC (hereafter, “Edwards”).

**Covered Entity.** “Covered Entity” shall mean Customer who issues a purchase order for the Services in the Underlying Agreement (hereafter, “Covered Entity”).

**Data Aggregation.** “Data Aggregation” shall have the meaning assigned to such a term in 45 CFR § 164.501, and includes, but is not limited to, combining PHI created or received by Edwards from covered entities to whom Edwards is a Business Associate to permit data analysis services for Covered Entity as set forth in the Underlying Agreement or an applicable statement of work or other written agreement and that is consistent with this BAA.

**Designated Record Set.** “Designated Record Set” shall have the meaning assigned to such term in 45 CFR § 164.501, but shall be limited to the collection or grouping of PHI that Edwards maintains, creates, or receives on behalf of Covered Entity.

**Electronic Protected Health Information (“EPHI”).** “Electronic Protected Health Information” or “EPHI” shall have the meaning assigned to such term in 45 CFR § 160.103, limited, however, to the information that Edwards maintains, creates, or receives on behalf of Covered Entity for the purposes of the Services.

**HIPAA.** “HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996, as modified and amended by the HITECH Act and other applicable laws, and its implementing

regulations, sometimes referred to as the “Privacy Rule,” “Security Rule,” and “Breach Notification Rule,” all as may be modified and amended from time to time.

**HITECH Act.** “HITECH Act” shall mean the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, enacted February 17, 2009, and any implementing regulations or guidance thereunder.

**Protected Health Information (“PHI”).** “Protected Health Information” or “PHI” shall have the meaning set forth in 45 CFR § 164.103, limited, however, to the information that Edwards creates, maintains, or receives on behalf of Covered Entity for the purposes of the Services. PHI includes EPHI.

**Secretary.** “Secretary” shall mean the Secretary of the Department of Health and Human Services.

**Services.** “Services” shall mean the provision of connectivity services and software focused on the transmission and delivery of near real-time and retrospective data for use in managing patients monitored with hemodynamic monitoring devices and the maintenance, update, and improvement of such services and software from time to time as set forth in the Underlying Agreement or an applicable statement of work or other written agreement and that is consistent with this BAA (collectively, the “Services”).

**Unsecured Protected Health Information (“Unsecured PHI”).** “Unsecured Protected Health Information” or “Unsecured PHI” shall have the meaning assigned to such term in 45 CFR § 164.402, limited however, to the information that Edwards creates, maintains, or receives on behalf of Covered Entity.

**Unsuccessful Security Incidents.** “Unsuccessful Security Incidents” shall mean Security Incidents that do not result in unauthorized access, use, disclosure, modification, or destruction of information or interference with system operation in an Information System in which PHI is stored or maintained, including, but not limited to: (i) “pings” and other broadcast attacks on an information system firewall; (ii) port scans; (iii) attempts to log on to an information system or enter a database with an invalid password or user name; or (iv) denial-of-service attacks that do not result in a server being taken offline, or any combination of the aforementioned, that does not result in unauthorized access, use, disclosure, modification, or destruction of Covered Entity’s EPHI.

## 2. **Business Associate Obligations.**

- (i) **Use and Disclosure.** Business Associate shall not use or disclose PHI other than (a) as necessary to perform the Services in accordance with the Underlying Agreement, (b) in accordance with Section 2(ii) of this Agreement, or (c) as Required by Law and in accordance with Section 2(iii) of this Agreement. Business Associate shall not use or disclose PHI in any manner that violates HIPAA or any other applicable federal or state laws and regulations relating to the privacy and security of PHI.
- (ii) **Certain Permitted Uses and Disclosures.** In accordance with 45 CFR §§ 164.504(e)(2)(i) and 164.504(e)(4), Edwards may use or disclose PHI (a) for the proper management and administration of Business Associate; (b) to provide Data Aggregation services for the Covered Entity; (c) in order to create de-identified PHI pursuant to 45

CFR §§ 164.514(b) and use the resulting de-identified data for its business purposes, provided that the de-identified data will not be associated with or attributable to Covered Entity or its employees or patients; and (d) to carry out the legal responsibilities of Business Associate; provided, however, that any permitted disclosure of PHI to a third party must be either Required By Law or subject to reasonable assurances obtained by Business Associate from the third party that the PHI will be held confidentially and used or further disclosed only as Required By Law or for the purposes for which it was disclosed to such third party, and that any breaches of confidentiality of the PHI which become known to such third party will be immediately reported to Business Associate.

- (iii) **Uses and Disclosures Required By Law.** Business Associate may use and disclose PHI to the extent such use or disclosure is Required By Law provided (a) the use or disclosure complies with and is limited to the relevant requirements of such law, (b) Business Associate promptly notifies Covered Entity of such use or disclosure and, at Covered Entity's request and Business Associate's expense, assists in obtaining a protective order or other similar order, and (c) the use or disclosure complies with the requirements of 45 CFR § 164.512 to the same extent such requirements would apply if the use or disclosure were made by Covered Entity.
- (iv) **Minimum Necessary.** Business Associate agrees to follow any guidance issued by the Department of Health and Human Services regarding what constitutes "minimum necessary" with respect to the use or disclosure of PHI, to the extent it is applicable to Business Associate's provision of the Services. Until the time that any such guidance is issued, Business Associate shall, where applicable and required by HIPAA, limit its use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of such use or disclosure.
- (v) **Safeguards.** Consistent with the requirements of 45 CFR § 164.504, Business Associate shall use appropriate administrative, technical, and physical safeguards to prevent the use or disclosure of PHI other than as permitted in this Agreement.
- (vi) **Security of EPHI.** Business Associate agrees to comply with the applicable standards of 45 CFR §§ 164.306, 164.308, 164.310, 164.312, 164.314, and 164.316 with respect to EPHI.
- (vii) **Notification Obligations.** Business Associate shall report to Covered Entity without unreasonable delay any Security Incident of which Business Associate becomes aware. In addition, Business Associate shall report to Covered Entity without unreasonable delay any acquisition, access, use or disclosure of Unsecured Protected Health Information not permitted by this Agreement. In no case shall such notification of the unauthorized acquisition, access, use or disclosure of unsecured PHI occur later than 15 calendar days after Business Associate's discovery. Discovery will be deemed to occur on the date that Business Associate actually became aware or, by exercising reasonable diligence should have been aware, of the unauthorized acquisition, access, use or disclosure of Unsecured PHI. To the extent an assessment by Business Associate concludes that a Breach of Unsecured PHI has occurred, such notification shall also include, to the extent possible and known to Business Associate, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed during the incident, along with any other information that

the Covered Entity will be required to include in its notification to the Individual, the media and/or the Secretary, as applicable, including, without limitation, (a) a description of the incident, (b) the date of the incident and the date of its discovery, (c) the types of Unsecured Protected Health Information involved, and (d) a description of Business Associate's investigation, mitigation, and prevention efforts. In the event that a Breach occurs that is properly attributable to the acts or omissions of Business Associate, Business Associate shall cooperate and assist Covered Entity in preparing any written notifications required by the Breach Notification Rule.

Notwithstanding the notification provisions above, the Parties acknowledge and agree that this **Section 2(vii)** constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of Unsuccessful Security Incidents for which no additional notice to Covered Entity shall be required.

- (viii) **Mitigation.** To the extent properly attributable to the acts or omissions of Business Associate, Business Associate shall mitigate promptly, to the extent practicable, any harmful effect that is known to Business Associate of an acquisition, access, use or disclosure of PHI by Business Associate in violation of this Agreement, the Privacy Rule, the Security Rule, or other applicable federal or state laws concerning the privacy or security of PHI. Business Associate shall promptly thereafter provide Covered Entity with a written report of the issues and corresponding actions taken by Business Associate.
- (ix) **Subcontractors.**
- a. **Written Agreement.** Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on its behalf agrees in writing to materially similar restrictions and conditions that apply to Business Associate with respect to such PHI under HIPAA, including without limitation the provisions of this Section 2.
- b. **Violations of Agreement.** If Business Associate becomes aware of a pattern of activity or practice of a Subcontractor that constitutes a material violation of the subcontractor's obligations under the written agreement described in **Section 2(ix)(a)**, Business Associate agrees to take reasonable steps to cure or end the violation, and if such steps are unsuccessful, to terminate the agreement, if feasible.
- (x) **Individual Rights.** The Parties agree and acknowledge that Business Associate will not through the provision of the Services, maintain PHI on behalf of Covered Entity that would be considered part of a Designated Record Set. Notwithstanding this acknowledgement, Business Associate agrees to undertake the following actions.
- a. **Request to Access or Amend PHI.** If any Individual submits a request to Business Associate for access to or amendment of his or her PHI in a Designated Record Set, Business Associate agrees to notify Covered Entity of such request and provide such information as known and reasonably available to Business Associate that may assist Covered Entity in its response to the request.

b. **Request for Accounting of Disclosures.** If any Individual submits a request to Business Associate for an accounting of disclosures of his/her/their PHI, Business Associate agrees to notify Covered Entity of such request and provide such information as known and reasonably available to Business Associate that may assist Covered Entity in its response to the request.

(xi) **Remuneration in Exchange for PHI.** Except as permitted under 45 CFR § 164.502(a)(5)(ii), Business Associate agrees that it shall not directly or indirectly receive remuneration in exchange for PHI from or on behalf of the recipient of such PHI.

(xii) **Audit.** Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, created or received by Business Associate on behalf of, Covered Entity available to the Secretary, upon request, for purposes of determining and facilitating Covered Entity's compliance with HIPAA.

### 3. **Covered Entity Obligations.**

(i) **Appropriate Permissions.** Covered Entity represents that it has provided all necessary notices to Individuals and has obtained any necessary permissions from Individuals and other entities, in order to disclose PHI to Business Associate and in order for Business Associate to use and disclose PHI as set forth in this BAA, in compliance with HIPAA and other applicable laws and regulations.

(ii) **Individual Permission.** Covered Entity shall notify Business Associate of change(s) in, or revocation of, permission by an Individual to use or disclose PHI, to the extent such change(s) affect(s) Business Associate's permitted uses or disclosures of PHI.

(iii) **Restrictions.** Covered Entity shall notify Business Associate of restriction(s) on the use or disclosure of PHI to which Covered Entity has agreed, to the extent such restriction(s) affect(s) Business Associate's permitted uses or disclosures of PHI.

### 4. **Term & Termination.**

(i) **Term.** The term of this Agreement shall begin on the effective date of the Underlying Agreement and shall terminate when all PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is returned to Covered Entity or destroyed, as agreed by the Parties. Business Associate may retain PHI as required by applicable law.

(ii) **Termination for Cause.**

a. **By Covered Entity.** Upon Covered Entity's knowledge of a material violation by Business Associate of this Agreement, Covered Entity may:

1. immediately terminate this Agreement and the Underlying Agreement if Business Associate has violated a material term of this Agreement and cure is not possible; or

2. terminate this Agreement and the Underlying Agreement upon thirty (30) days' notice after (1) Covered Entity determines that Business Associate has violated a material term of this Agreement, and (2) following Covered Entity's written notification of the material violation to the Business Associate, Business Associate is unable or unwilling to take steps to cure the violation within such thirty (30) day period. In the event Business Associate cures the violation within such thirty (30) day period, this Agreement shall remain in full force and effect.

b. **By Business Associate.** Upon Business Associate's knowledge of a material violation by Covered Entity of this Agreement, Business Associate may:

1. immediately terminate this Agreement and the Underlying Agreement if Covered Entity has violated a material term of this Agreement and cure is not possible; or

2. terminate this Agreement and the Underlying Agreement upon thirty (30) days' notice, after (1) Business Associate determines that Covered Entity has violated a material term of this Agreement, and (2) following Business Associate's written notification of the material violation to Covered Entity, Covered Entity is unable or unwilling to take steps to cure the violation within such thirty (30) day period. In the event Covered Entity cures the violation within such thirty (30) day period, this Agreement shall remain in full force and effect.

(iii) **Survival.**

a. In the event of termination of this Agreement pursuant to Section 4(ii), to the extent feasible, Business Associate shall return to Covered Entity or destroy all PHI that Business Associate still maintains in any form. If the return or destruction of all PHI is not feasible, Business Associate shall extend the protections of this Agreement to the remaining information and limit further use and disclosure of PHI to those purposes that make the return or destruction of the PHI infeasible.

b. The terms of Section 2(vii) ("Notification") and Section 2(viii) ("Mitigation") along with such other terms that by their nature indicate the intent for survival, shall survive the termination or expiration of this Agreement.

5. **Miscellaneous.**

(i) **Notices.** All notices to be made under this BAA shall be given in writing (with a copy via email if email address is provided below) and shall be deemed to have been duly given if delivered by U.S. Postal Service, prepaid, certified or registered mail, return receipt requested, or regionally recognized overnight service and notice deemed given on the day delivered, as evidenced by the courier's receipt to the other Party at the addresses referenced below:

If to Covered Entity, to: Address identified in the applicable Quote for Services  
Attn: Legal Department/Privacy Officer

If to Business Associate, to: Edwards Lifesciences LLC  
Attn: Privacy Officer  
One Edwards Way  
Irvine, CA 92614  
Email: [privacy@edwards.com](mailto:privacy@edwards.com)

- (ii) **Compliance with Laws.** The Parties shall comply with all applicable federal, state and local laws, rules and regulations concerning the privacy and security of PHI, including, without limitation, the requirements of HIPAA.
- (iii) **Underlying Agreement.** Except as specifically required to implement the purposes of this BAA, to the extent inconsistent with this BAA, all terms of the Underlying Agreement shall remain in full force and effect. In the event of a conflict between the terms of the Underlying Agreement and this BAA, this BAA shall control.
- (iv) **Amendment.** The Parties acknowledge that the Secretary may promulgate additional regulations and interpretative guidance that is not available at the time of executing this Agreement. In the event Covered Entity determines in good faith that any such regulation or guidance adopted or amended after the execution of this Agreement is required by law to be implemented and made a part hereof, this Agreement shall be renegotiated in good faith so as to amend the applicable provision(s) in a manner that would eliminate any such substantial risk.
- (v) **Regulatory References.** A reference in this BAA to a section in HIPAA means the section as in effect or as amended, and for which compliance is required.
- (vi) **Interpretation.** Any ambiguity in this BAA shall be resolved in favor of a meaning that permits the Parties to comply with HIPAA.
- (vii) **Choice of Law.** This BAA shall be deemed to have been made in the state of California, and the validity, interpretation and performance of this BAA shall be governed by, and construed in accordance with, the internal law of the state of California, without giving effect to the conflict of law principles thereof, to the extent not preempted by applicable federal law. For purposes of all claims arising out of or relating to this Agreement, each of the Parties hereby irrevocably submits to the exclusive jurisdiction of the state and federal courts located in Orange County, California.
- (viii) **Binding Effect.** This BAA shall be binding upon, and shall inure to the benefit of, the Parties and their respective successors and permitted assigns.
- (ix) **Legal Actions.** Promptly, and in any case no later than five (5) business days after notice thereof, Business Associate shall advise Covered Entity of any actual or potential

action, proceeding, regulatory or governmental orders or actions, or any material threat thereof that becomes known to it that may affect the interests of Covered Entity or jeopardize this Agreement, and of any facts and circumstances that may be pertinent to the prosecution or defense of any such actual or potential legal action or proceeding, except to the extent prohibited by law.

- (x) **Notice of Request or Subpoena for Data.** Business Associate agrees to notify Covered Entity immediately, but in any case, no later than three (3) business days after Business Associate's receipt of any request or subpoena for PHI or an accounting thereof, not otherwise provided in this Agreement. Business Associate shall promptly comply with Covered Entity's instructions for responding to any such request or subpoena, unless such Covered Entity instructions would prejudice Business Associate. To the extent that Covered Entity decides to assume responsibility for challenging the validity of such request, Business Associate agrees to cooperate fully with Covered Entity in such challenge. The provisions of this Section shall survive the termination of this Agreement.
- (xi) **Requests from Secretary.** Immediately, but in any case, no later than five (5) business days after notice thereof, Business Associate shall advise Covered Entity of any inquiry by the Secretary concerning any actual or alleged violation of HIPAA. Business Associate agrees to permit Covered Entity to respond to any such notice or inquiry. Business Associate shall cooperate fully with Covered Entity in responding to any such inquiry.
- (xii) **Additional Privacy and Security Compliance.** Business Associate acknowledges that applicable HIPAA provisions directly apply to Business Associate and its subcontractors. Such requirements are incorporated by reference as if fully set forth herein.
- (xiii) **Property Rights in PHI.** Business Associate hereby acknowledges that, as between Business Associate and Covered Entity, all PHI shall be and remain the sole property of Covered Entity, including any forms of PHI developed by Business Associate in the course of fulfilling its obligations under this Agreement.
- (xiv) **Representations and Warranties.** Business Associate represents and warrants that no PHI has been transferred by Business Associate to third Parties in violation of state or federal privacy laws. There are no suits, notices, claims, investigations, orders or proceedings currently pending, or, to the knowledge of Business Associate, threatened, by state or federal agencies, or private parties involving notice or information to Individuals that PHI held or stored by the Business Associate has been compromised, lost, taken, accessed or misused. Business Associate further represents and warrants that it is not currently under any agreement, including any settlement agreement or consent decree, with the Office of Civil Rights of the U.S. Department of Health and Human Services involving creating, receiving, maintaining, or transmitting PHI
- (xv) **Third Party Beneficiaries.** This Agreement does not create any third-party beneficiary rights.

- (xvi) **Assignment.** This BAA shall not be assigned by either party without the prior written consent of the other party, except that Business Associate may assign this BAA to an Affiliate or successor to all or substantially all of the business to which this BAA is related without the consent of Covered Entity. “Affiliate” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control” for purposes of this definition, mean direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity.
- (xvii) **Headings.** Section headings contained in this Agreement are included for convenience only and are not to be used in construing or interpreting this Agreement.
- (xviii) **Counterparts; Electronic Signatures.** This Agreement may be executed in any number of counterparts, each of which need not contain the signature of more than one Party, but all such counterparts taken together shall constitute one and the same agreement. Electronic signatures in portable document format (“.pdf”) shall be binding upon the Parties and shall have the same force and effect as manual signatures.
- (xix) **Authority to Execute.** The signatories to this Agreement represent and warrant that they are duly authorized to execute this Agreement on behalf of the Party that they purport to represent.

## EXHIBIT C

### SERVICE LEVEL STANDARDS

#### Issue Resolution

Edwards will use commercially reasonable efforts to promptly respond to requests for support, either through electronic mail (tech\_support@edwards.com) or by telephone (1-800-822-9837), in accordance with the following time periods.

Priority Level	Description	Response Time
Level 1	The entire Service is not working	4 business hours
Level 2	A major component of the Service is not working that materially restricts the user or performance of the Service	24 business hours
Level 3	A minor component of or enhancement to the Service is not working but is only causing a minor impact on use of the Service	Within 1 week
Level 4	A problem that does not restrict the operation of the Service	At Edwards discretion

Edwards shall act in good faith to determine the priority level of each problem. Response times are defined as the period between the receipt of the request and the initial response to the user making such request. Upon issue resolution, Edwards shall use a reasonable method to provide users with an update of such resolution.

#### Service Commitment

The uptime of the Service shall be at least 99.5%, measured monthly, excluding holidays and weekends and scheduled maintenance. Most months, this means Customer should expect no more than approximately 30 minutes of downtime. If Customer requests maintenance during available hours, any uptime or downtime calculation will exclude periods affected by such maintenance. Further, any downtime resulting from outages of third-party connections or utilities or other reasons beyond Edwards' control will also be excluded from any such calculation.

Downtime shall begin to accrue as soon as Customer (with notice to Edwards) recognizes that downtime is taking place, and continues until the availability of the Services is restored.

## EXHIBIT D

### INFORMATION SECURITY PRACTICES FOR THE VIEWFINDER NETWORK

#### 1. Introduction

##### 1.1. Purpose.

1.1.1. This document describes the Edwards information security practices and policies (“Infosec Requirements”) for handling of data and electronic protected health information (“ePHI”) within the Viewfinder network as of the Effective Date of the Edwards Viewfinder Subscription Agreement (the “Agreement”).

1.1.2. Edwards will comply with these Infosec Requirements during the term of the Agreement and for any period of time thereafter during which Edwards has access to Customer Data that includes ePHI.

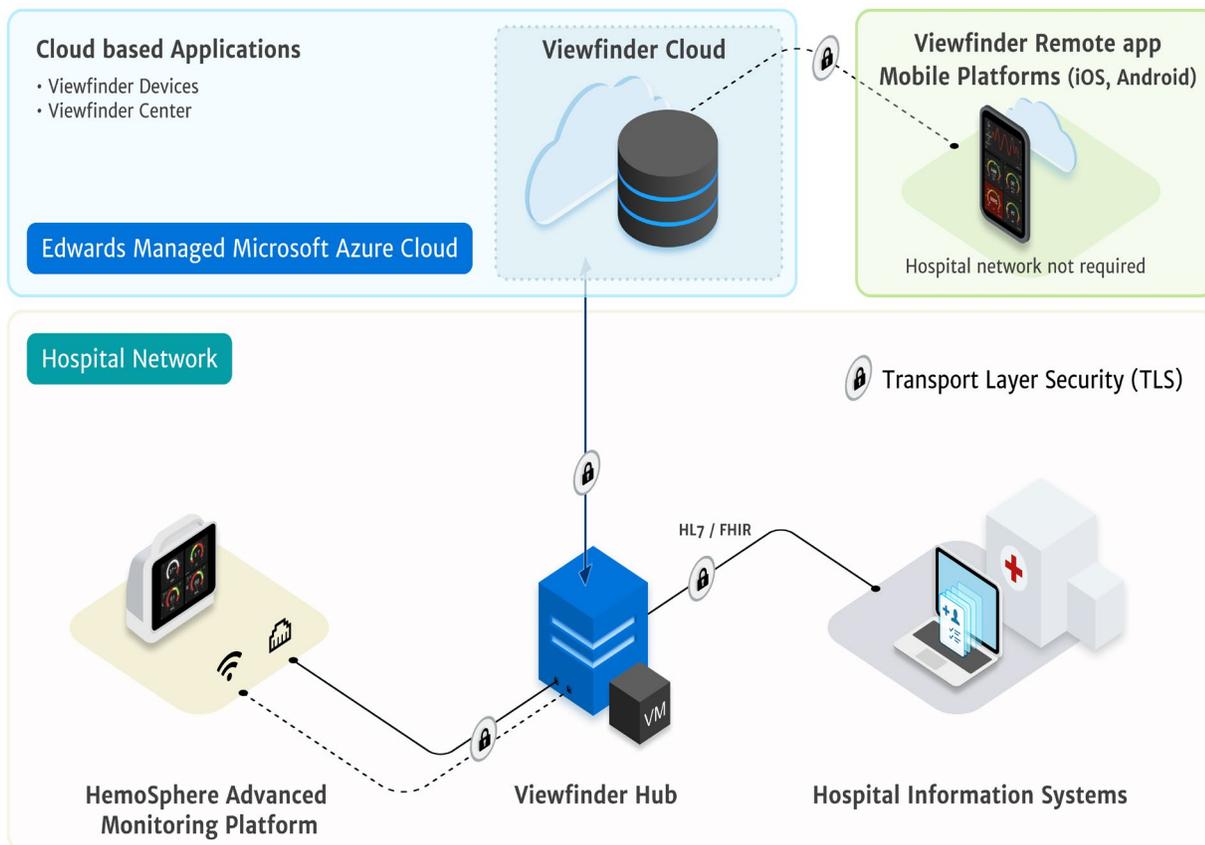
##### 1.2. Scope.

1.2.1. These Infosec Requirements apply to the Edwards Viewfinder network. The network includes the Viewfinder remote mobile application, the Viewfinder hub, and the Edwards Viewfinder cloud.

1.2.2. Capitalized terms used in these Infosec Requirements have the respective meanings given to them in the Agreement.

#### 2. Viewfinder data flow

2.1. Generally. The Viewfinder hub is a secure data exchange software hub, installed on a hospital server, that serves as the pipeline for the secure exchange of data collected from the Edwards HemoSphere advanced monitoring platform and relayed to the Viewfinder cloud and any configured hospital IT systems like Electronic Medical Record (EMR) systems. The Viewfinder cloud processes and securely transmits the data to the Viewfinder remote app, which enables a near-real-time remote display of hemodynamic parameters from a connected HemoSphere monitor.



## 2.2. Viewfinder hub.

2.2.1. The Viewfinder hub is an Ubuntu Linux based virtual appliance deployed either on a hospital server, or on VMware / Hyper-V hypervisor virtual machine provided by the hospital. Viewfinder Hub deployments will be managed and maintained by Edwards personnel.

2.2.2. The hub runs on the Ubuntu 18.04 operating system and Docker OS-level virtualization platform for containerized applications.

2.2.3. The hub connects to HemoSphere monitor(s) via a LAN or wireless connection and transmits hemodynamic data to the Edwards Viewfinder cloud over the hospital and external networks.

2.2.4. Data stored at rest on the Viewfinder hub is encrypted using AES 256 encryption.

2.2.5. Data transmitted via the Viewfinder hub contains timestamped hemodynamic measurements, but no patient information.

2.2.6. The data gathered by the Viewfinder hub is transmitted to cloud over MQTT with mTLS 1.2 and HTTP with mTLS 1.2 connections. The connections are secure, mutually authenticated, and encrypted.

### 2.3. Viewfinder cloud.

2.3.1. The Viewfinder cloud stores PHI data in an Azure SQL Database dedicated per hospital tenant. De-identified, monitored data is stored in Azure blob storage.

2.3.2. Data is transmitted to the Viewfinder remote mobile application over TLS 1.2.

2.3.3. Authentication and user management from the Viewfinder remote user side is maintained through MFA and OAuth 2.0 flows.

## 3. **General security measures.**

3.1. Edwards employs the following measures to protect the Viewfinder network:

3.1.1. All connections between system components (Viewfinder hub, Viewfinder cloud, Viewfinder remote) are authenticated, encrypted, and protected using TLS 1.2.

3.1.2. Mutual TLS is maintained whenever possible. When it is not possible, client authentication is performed through user multifactor authentication (MFA) and digitally signed JSON Web Token (JWT).

3.1.3. All data stored at rest is encrypted using AES 256 cipher. Encryption is provided by Transparent Data Encryption (TDE), which is supplemented with application-level encryption for sensitive data.

3.1.4. All data in transit is encrypted using AES 256 cipher as part of TLS 1.2 exchange.

3.1.5. All user interfaces are protected using MFA, OAuth 2.0 Session Management, and JWT token-based authorization.

3.1.6. All network traffic into and out of the Viewfinder cloud is routed through Web Application Firewall (WAF) and Next Generation Firewall (NextGen)

3.1.7. Azure Security Center, CrowdStrike EDR, and Prisma Cloud solutions are used to provide runtime security.

3.1.8. The Azure Monitor/Azure Sentinel framework is used to provide incident detection and response.

### 3.2. Additional solution security features include:

- 3.2.1. Industry standard processes and technology to detect and remediate software viruses and other malware on all systems used to access, process, or host the Viewfinder network.
- 3.2.2. File integrity monitoring
- 3.2.3. Regular testing against OWASP top ten vulnerabilities
- 3.2.4. Strong authentication, session management, authorization
- 3.2.5. OS hardening for platforms used to process, store, or host the Viewfinder network or Customer Data
- 3.2.6. Network segmentation, to limit the effect of any security compromise
- 3.2.7. Applying the principle of least privilege when assigning access to the Viewfinder network

## 4. Log management

### 4.1. Maintenance.

- 4.1.1. Security logs are maintained in Azure Sentinel for a duration of 90 days. During that time, no individual has the rights to delete the logs.
- 4.1.2. Logs are archived after 90 days and are maintained, in read-only form, for one year.

### 4.2. Review.

Logs are reviewed continuously through automated systems. Alerts are sent to administrators if suspicious activity is detected.

### 4.3. Logged data. Logs track the following:

- 4.3.1. Unique user ID, unique data subject ID, function performed, and date/time the event was performed for Azure service changes and configuration.
- 4.3.2. The activities of privileged users (administrators, operators, etc.), including the success/failure of the event, time the event occurred, the account involved, the processes involved, and additional information about the event.
- 4.3.3. Faults related to problems with information processing or communications systems and other errors

- 4.3.4. Next Generation and Web Application Firewalls logs
- 4.3.5. Identity Access Management (Azure Active Directory) logs
- 4.3.6. Run-time detection logs and streams (Prisma Cloud, CrowdStrike, Azure Security Center).

## 5. User management

### 5.1. Access.

- 5.1.1. Access to the Viewfinder network is managed by Edwards' administrators using a third-party identity management system (Azure Active Directory).
- 5.1.2. Viewfinder Network supports federating to Hospital Identity Management systems that support OAuth 2.0.
- 5.1.3. Alternately, hospitals can choose to utilize user management functionality provided by Viewfinder Network.
- 5.1.4. New end users are required to utilize multi-factor authentication.

### 5.2. Security measures.

- 5.2.1.1. Customers that choose to utilize Viewfinder Network user management functionality will have to adhere to the following password management policy:
  - 5.2.1.1.1. Passwords must have a minimum length of ten (10) characters and strong complexity.
  - 5.2.1.1.2. Reuse of [*last 10*] passwords is prohibited.
  - 5.2.1.1.3. Account lockout after no more than [10] consecutive failed authentication attempts.
- 5.2.1.2. All accounts are required to use multi-factor authentication.
- 5.2.1.3. Authorization is managed through digitally signed JWT tokens.
- 5.2.1.4. Session integrity and termination is managed through OAuth 2.0 flows.

## 6. Database

- 6.1. The data for the Viewfinder network is stored in an Edwards managed cloud hosted databases on Microsoft Azure.
- 6.2. Each hospital tenant has a separate dedicated PHI database for purposes of tenant isolation.
- 6.3. All databases are behind Next Generation Firewall and not directly accessible to the internet.
- 6.4. All communications with databases are protected using AES-256 encryption as part of mutually authenticated TLS 1.2 connection.
- 6.5. All data stored in PHI databases is encrypted at rest utilizing AES-256 cipher.
- 6.6. All secrets related to encryption or authentication are stored in a key vault instance unique per hospital tenant.

## 7. Firewalls

All Viewfinder business logic and databases deployed in cloud are protected by NextGen Firewall and Web Application Firewall. All network traffic into and out of the Viewfinder cloud is routed through these firewalls.

## 8. Systems development

### 8.1. Solution requirements.

- 8.1.1. All solution requirements are documented in a software requirement specification.
- 8.1.2. Edwards software engineers develop the solution according to the software requirements specification.
- 8.1.3. An independent team of testers conducts verification testing to confirm that the requirements have been met.
- 8.1.4. Confidential Edwards test data are adequately protected, controlled, and removed from environments used for development and testing.
- 8.1.5. All changes to the production environment require approval by a cross-functional team in a formal design review or change board. Risks are identified, evaluated, and addressed according to strict internal procedures.

8.1.6. Access to code and the development and production environments is secured rigorously and is only possible from the Edwards internal network, subject to passing MFA, and, in case of the production environment, only from specially dedicated, hardened machines.

## 8.2. Code security.

8.2.1. All production code is digitally signed, using trusted third-party Public Key Infrastructure (PKI) services.

8.2.2. As part of Edwards' CI/CD pipeline, code is scanned nightly for vulnerabilities, both third-party and any introduced in Edwards custom code. This scanning is performed using best in class Software Composition Analysis (SCA) and Static Application Security Testing (SAST) tools, which allows for deep and thorough analysis as well as continuous vulnerabilities detection.

8.2.3. Dynamic Application Security Testing (DAST) is executed on live, deployed application instances

8.2.4. A trusted third-party penetration team is contracted to perform continuous penetration testing on the product (including milestones).

8.2.5. Any vulnerabilities discovered are triaged and run through an internal risk assessment with enforced remediation of all Critical and High vulnerabilities discovered.

## 9. **Edwards access to ePHI**

### 9.1. Generally.

9.1.1. By policy, Edwards prohibits access to ePHI except for technical, administrative or debugging purposes.

9.1.2. No ePHI may be stored anywhere outside of the dedicated Azure environment or extracted out of it.

### 9.2. Access restrictions.

9.2.1. Access to ePHI is restricted.

9.2.1.1. Stored PHI is encrypted.

9.2.1.2. Database administrator and Key Vault administrator roles are segregated.

9.2.2. When access to ePHI is required and permitted, access is restricted to:

9.2.2.1. A small number of named technical and clinical support personnel.

9.2.2.2. Special security-hardened workstations as a jump to JIT VM, spanned in the production environment.

9.2.3. Access to the production environment is restricted.

9.2.3.1. Only dedicated Edwards IT and security professionals are permitted access.

9.2.3.2. Access is limited to Edwards' internal network and only from dedicated, hardened workstations.

9.2.3.3. Access credentials are managed by Privileged Access Management tool and are rotated on less than daily basis.

## **10. Key management**

10.1. Encryption keys and similar secret information are stored and managed using a dedicated-to-tenant (hospital) instance of cloud secrets management system (Azure Key Vault).

10.2. All certificates issued in the system are signed by a trusted third-party PKI. Signing keys are securely stored at Hardware Security Modules (HSMs), behind multiple physical security controls, and protected by PKI vendor.

10.3. Access to any of these environments is only open for small group of dedicated Edwards IT and Security professionals from hardened machines.

## **11. Information security program**

11.1. Generally.

11.1.1. Edwards maintains a formal, written information security policy that it communicates to all employees and contractors. The policy specifies practices for the acceptable use of computing resources and data.

11.1.2. Edwards will provide its information security policy to Customer for review upon request and subject non-disclosure agreement.

11.1.3. The information security policy includes the following:

- 11.1.3.1. Access controls.
- 11.1.3.2. Security awareness training.
- 11.1.3.3. Vulnerability/patch management.
- 11.1.3.4. Risk management.
- 11.1.3.5. Configuration management.
- 11.1.3.6. Asset disposal policies.
- 11.1.3.7. Incident response measures.
- 11.1.3.8. Disaster recovery plans, which are tested at least once annually.
- 11.1.3.9. Change management processes for critical systems.

11.1.4. Edwards uses commercially reasonable efforts to keep its information security practices current, based upon changes in applicable law, best practices, and industry standards.

## **12. Third-party assessments**

12.1. HITRUST. Edwards is currently in the process with a third-party assessor of becoming HITRUST-certified for the Viewfinder network. HITRUST certification requires compliance with the HITRUST Common Security Framework which is based on nationally and internationally accepted standards including ISO, NIST, PCI and HIPAA to ensure a comprehensive set of baseline security controls.

12.2. Business Associate Agreement.

12.2.1. Edwards also maintains a subcontractor BAA with cloud hosting provider, Microsoft.

12.2.2. Microsoft maintains SOC-1 Type II and HITRUST certifications for its Azure platform, which hosts the Viewfinder cloud.

## **13. Incident management and notice**

13.1. Edwards maintains and follows a documented security incident response plan.

13.2. In the event of an incident that is reasonably likely to compromise Customer Data under Edwards’ control, Edwards agrees to do the following:

13.2.1. notify Customer in accordance with the incident classification, contacts, and timing described in Attachment 1.

13.2.2. Designate a point of contact who will initiate and manage regular incident status calls between Customer, Edwards, and any other involved parties, as appropriate.

**14. Business continuity**

14.1. Edwards will back up its applications, data, and software on a regular basis

14.2. All supporting infrastructure for the Viewfinder network and data are available and supported in a managed disaster recovery program that includes storage capacity, processing power, points of presence, and backup power.

**ATTACHMENT 1: Incident notice requirements**

INCIDENT	CONTACTS	TIMING
Security Breach affecting Customer Data, systems containing Customer Data, or systems that directly interact with systems containing Customer Data	<b>Edwards contacts:</b> <a href="mailto:privacy@edwards.com">privacy@edwards.com</a>  Product_security@edwards.com  <b>Customer contacts:</b> Address identified in the applicable quote for Services Attn: Legal Department	Within 48 hours of Edwards’ confirmation of the Security Breach

“Security Breach” shall mean (A) any event for which applicable law requires notification of such event to be given to affected parties or another activity in response to the event; or (B) any actual or attempted compromise of systems security that is reasonably likely to result in unauthorized access, acquisition, processing, use, or disclosure of Customer Data that is in the control of Edwards or its contractors in connection with the Viewfinder network.