



## Cepheid C360 Terms and Conditions

Last Updated October 18, 2021

THESE CEPHEID C360 TERMS AND CONDITIONS (“**C360 AGREEMENT**”) GOVERN THE USE OF CEPHEID C360 SOFTWARE, WEB APPLICATIONS, AND ANY ASSOCIATED CEPHEID INTERFACES AND APIS (COLLECTIVELY REFERRED TO AS THE “**SOFTWARE**”) BY THE CUSTOMER (“CUSTOMER”, “USER”, “YOUR”, “YOU”) THAT EXECUTED OR OTHERWISE ENTERED INTO A PRODUCT AGREEMENT (DEFINED BELOW) WITH CEPHEID (DEFINED BELOW) THAT REFERENCES THIS C360 AGREEMENT, OR CLICKED A BOX OR OTHERWISE INDICATED ACCEPTANCE, OR USES THE SOFTWARE. CUSTOMER AND CEPHEID MAY BE REFERRED TO HEREIN AS “**PARTY**”, OR COLLECTIVELY “**PARTIES**”.

BY EXECUTING OR OTHERWISE ENTERING INTO THE PRODUCT AGREEMENT THAT REFERENCES THIS C360 AGREEMENT, OR CLICKING A BOX OR OTHERWISE INDICATING ACCEPTANCE OR USING THE SOFTWARE, YOU AGREE TO THE TERMS OF THIS C360 AGREEMENT. THE EFFECTIVE DATE (“**EFFECTIVE DATE**”) OF THIS AGREEMENT IS THE EFFECTIVE DATE OF THE PRODUCT AGREEMENT. IN CASE OF ACCEPTANCE BY CLICKING A BOX, THE EFFECTIVE DATE OF THIS AGREEMENT SHALL BE WHEN CEPHEID APPROVES THE ACCEPTANCE IN WRITING.

BY AGREEING TO THESE TERMS ON BEHALF OF AN ORGANIZATION, YOU AGREE THAT YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON ORGANIZATION’S BEHALF AND THAT CUSTOMER, AS USED HEREIN, REFERS TO YOUR ORGANIZATION.

THIS C360 AGREEMENT DOES NOT APPLY TO (A) THE CUSTOMERS LOCATED OUTSIDE OF THE UNITED STATES TERRITORY AND CANADA AND (B) PERSONAL DATA (DEFINED BELOW) RELATES TO INDIVIDUALS LOCATED OUTSIDE OF THE UNITED STATES TERRITORY AND CANADA, INCLUDING THE EUROPEAN ECONOMIC AREA.

The Software provides Internet services, including management, aggregation, sharing, alerting, and reporting data from Cepheid’s compatible and connected systems, including the Cepheid Systems (defined below). In some instances, additional software may be required to connect the Cepheid Systems to the Software. This additional software may be licensed under a separate license agreement.

### 1. Definitions

“**Administrator**” means a single User employee, designated by the User, who configures, manages and uses the Software.

“**Applicable Privacy Laws**” means the privacy and data protection legislation and regulations in force during the Term applicable to Personal Data (defined below) processed under this Agreement.

“**Authorized Users**” means the User’s employees or agents authorized by the User to use the Software or access data via the Software in accordance with this C360 Agreement, and for whom the User shall remain responsible and liable.

“**C360 Data**” means data collected by your Cepheid Systems and transmitted by and to the Software, or any data that may be generated or encountered through use of the Software.

“**Cepheid**”, “**we**”, “**us**”, or “**ours**” mean the California corporation with a principal place of business is at 904 E. Caribbean Drive, Sunnyvale, CA 94089, U.S.A., including its subsidiaries.

“**Cepheid Service Provider**” means our vendors, contractors, sub-contractors, business and service partners, developers, or other third parties that perform services for, on behalf of or jointly with Cepheid.



“**Cepheid Systems**” includes the GeneXpert family of systems which are comprised of analytical equipment, computers, including hubs and mobile devices, and software controlling the analytical equipment.

“**Confidential Information**” means any non-public information disclosed or made available directly or indirectly by one Party (the “**Discloser**”) to the other Party (the “**Recipient**”) in connection with this C360 Agreement, however such information is disclosed, including, without limitation, in writing, orally or electronically. Cepheid’s Confidential Information includes, without limitation, the Software and its functionality, usability and performance, and the Documentation.

“**Documentation**” means any Cepheid technical and other information such as the C360 Analytics Institution Administrator Manual, C360 Analytics Quick Reference Guide, C360 Sync Installation Instructions, C360 Sync Quick Reference Guide, C360 Sync Network Connectivity Guide, C360 Admin Manual, and any other user or administrative support materials that Cepheid provides to you, and any analytics, reports or documentation produced by Cepheid and/or made available to you via the Software or otherwise.

“**Intellectual Property Rights**” means copyright, patents, trademarks, design rights, database rights, trade secrets, know-how and all other similar rights anywhere in the world whether or not registered, including applications for any of the foregoing rights, as applicable.

“**Lab User**” means an Authorized User that operates the Cepheid Systems.

“**Malware**” means viruses, malware or any other thing or device (such as software, code, file or program) including worms, trojan horses, viruses and other devices.

“**Personal Data**” as used herein, shall have the same meanings given in the Applicable Privacy Laws (which may be regarded as personal data or personal information therein). If Personal Data (or personal information) is not defined in the Applicable Privacy Laws, it shall mean any information that relates to an identified or identifiable natural person; an identifiable natural person being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. .

“**Product Agreement**” means the agreement entered into between Customer and Cepheid pursuant to which Customer acquires or has acquired use of or service for the Cepheid Systems, or other Cepheid products or services, and references to this C360 Agreement, including, without limitation, Cepheid quotes, purchase orders, order forms, and letter agreements.

“**User Data**” means the data provided by you or by Authorized Users, which is accessed or transmitted by the Software, which may include Personal Data.

## 2. Term

2.1 This Agreement commences on the Effective Date and will continue in force unless terminated as permitted below or superseded by written mutual agreement of the Parties.

## 3. Ownership

3.1 We own or are permitted to use all Intellectual Property Rights in our systems, including the Cepheid Systems, the Software, and the Documentation. The Software and all Intellectual Property Rights licensed to you under this C360 Agreement remain our property or that of our licensors.

## 4. License

4.1 Subject to your compliance with the terms and conditions of this C360 Agreement, we grant you a limited, non-exclusive, non-sub-licensable, non-transferable license to access and use the Software and Documentation, solely for your internal use during the Term and as permitted in this C360 Agreement.



## 5. Software

- 5.1 In consideration of your undertakings as set forth in this C360 Agreement, we will provide you with access to the Software and Documentation for use during the Term. The Software shall substantially conform to the descriptions provided in the Documentation.
- 5.2 We will provide access to the Software to the Administrator using a username and password system. The Administrator may create multiple Authorized User accounts.

## 6. Your Responsibilities

6.1 You shall:

- (a) provide us with all necessary cooperation in relation to this C360 Agreement and access to such information as we require to enable proper operation of the Software, including but not limited to User Data;
- (b) comply with all applicable laws and regulations with respect to your activities under this C360 Agreement; and
- (c) ensure that your network and systems are appropriate for your use of the Software.

6.2 You agree that you shall not (and shall ensure that your Authorized Users do not):

- (a) sublicense your rights in the Software, Documentation, or any other Intellectual Property Rights licensed to you under this C360 Agreement, or grant or purport to grant to any third party any right in or to same; or
- (b) allow access or use of the Software, Documentation, or any other Cepheid Confidential Information by anyone other than your Authorized Users, existing employees or agents, who are bound by confidentiality obligations at least as restrictive as those in this C360 Agreement.

6.3 In accordance with your internal policy, you undertake that you, the Administrator and each Authorized User, shall keep a secure password for their use of the Software, that such password will be changed regularly to ensure its security and to ensure that the Administrator and each Authorized User shall keep their password confidential. You shall take reasonable steps to ensure that the Administrator and all Authorized Users shall not access, store, distribute or transmit any Malware which may adversely affect: (i) the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; (ii) access to or the operation of any program or data, including the reliability of any program or data; (iii) the confidentiality, security, integrity, or availability of data, or (iv) the user experience. We reserve the right, without liability or prejudice to our other rights, to temporarily disable your access to the Software in the event that Malware is introduced by you or your Administrator or Authorized Users until the problem is resolved.

6.4 You shall not, and you shall ensure that the Authorized Users shall not, directly or indirectly:

- (a) modify, reverse engineer or attempt to obtain any source code or create derivative works of the Software or Documentation;
- (b) use the Software, Documentation and/or any other Cepheid Confidential Information to build a similar or competitive product or service; or



(c) use the Software, Documentation and/or any other Cepheid Confidential Information in a manner inconsistent with applicable law or this C360 Agreement.

6.5 Unless otherwise stated in the agreement under which you obtained the Cepheid Systems, you are responsible (at your cost) for providing secured Internet access and a secure site environment for and operation of the Cepheid Systems, and for integrating the Software with your existing systems and servers during the Term.

6.6 Software is not a data back-up or storage service and should be considered nonpersistent. You are responsible for keeping back-ups of your data processed on your behalf in connection with the Software (including C360 Data, User Data and any Personal Data contained in them).

6.7 If requested by Cepheid, you agree to provide feedback to us regarding your experiences with the Software, the Documentation, training, sign up, and support at mutually agreeable times and in formats as we may reasonably request.

## **7. Fees**

7.1 The Software and Documentation under this C360 Agreement are being provided to you at no cost during the Term as defined in Clause 2.1.

## **8. Termination**

8.1 We may terminate this Agreement for any reason or no reason, upon thirty (30) days' prior written notice to you.

8.2 You may terminate this C360 Agreement for any reason or no reason upon ninety (90) days' prior written notice during declared national emergency due to a pandemic. If there is no national emergency, or upon declaration that a pandemic is no longer a national emergency, you may terminate this C360 Agreement for any reason or no reason upon thirty (30) days' prior written notice to us.

8.3 Either Party may terminate this C360 Agreement immediately upon giving written notice to the other Party if:

- (a) the other Party is in breach of any of the terms of this C360 Agreement and such breach is incapable of being remedied;
- (b) the other Party is in breach of any of the terms of this C360 Agreement and, the breach being remediable, fails to remedy the breach within thirty (30) days from the date of a written request to do so; or
- (c) the other Party files or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency law.

8.4 Termination of this C360 Agreement shall not affect a Party's accrued rights and remedies.

8.5 On termination of this C360 Agreement, you shall immediately take necessary steps to disable the connection between your Cepheid Systems and the Software and cease using the Software, and shall promptly destroy or return the Documentation to us.



8.6 Prior to termination of this C360 Agreement, you may save User Data using the export functionalities provided in the Software and described in the Documentation. Upon termination of this C360 Agreement, we may, subject to our rights set out in Clauses 9.2, 9.3 and 9.5 destroy or otherwise dispose of any of the User Data in our possession unless we receive, no later than ten (10) days after the effective date of the termination of this C360 Agreement, a written request to support you in exporting the then available User Data. We shall use reasonable commercial endeavors to deliver the support to you within thirty (30) days of receipt of such a written request. Unless otherwise agreed, you shall pay all reasonable expenses incurred by us in providing such support.

## 9. Data Processing

9.1 The current fields in each data category of C360 Data as of the Effective Date of this C360 Agreement are shown in Exhibit A. These data fields and categories are subject to change by Cepheid in its sole discretion without any notice to you. As the Software functionality changes, additional data may be required.

9.2 You acknowledge and agree that during and after the Term, as applicable, we may:

- (a) Use C360 Data, including User Data, to support your use of the Software, Cepheid Systems and Cepheid's products and services;
- (b) Use C360 Data, including User Data, to improve and enhance our products or services, or develop new products and services; and
- (c) aggregate and/or de-identify C360 Data, including User Data, combine with other data we obtain, use or disclose to others the aggregated and/or de-identified data. We shall not attempt to re-identify the de-identified data, and at reasonable intervals, we shall test and evaluate the effectiveness of our technical and organizational measures to ensure the de-identification process is secure.

9.3 Without your authorization and except as expressly stated in this Agreement, BAA (defined below) or DPA (defined below), we will not share the C360 Data, including User Data, with others outside of our subsidiaries, parent or sister companies, or the Cepheid Service Providers unless:

- (a) it is de-identified (to the extent allowed by Applicable Privacy Laws) or aggregated;
- (b) we are required by law or regulation, or we reasonably believe that disclosure is necessary to comply with applicable laws and regulations, or to comply with a legal process or request;
- (c) we reasonably believe that it is appropriate or necessary to take precautions against liability or to protect the rights or safety of us, you, third parties, or the public;
- (d) we reasonably believe that it is appropriate or necessary to detect, prevent or otherwise address security, fraud or technical issues, or
- (e) it is necessary if we are acquired by or merged with a third-party entity, in which case, we reserve the right to transfer or assign the C360 Data, including User Data, as part of such merger, acquisition, sale, or other change of control.

9.4 To the extent that the data described in Clause 9.1 and Exhibit A contains any Personal Data, you and we acknowledge and agree that:

- (a) you are responsible (i) for ensuring that the collection, processing and sharing of such Personal Data in the context of your use of the Software complies with the requirements of applicable laws and



regulations, including Applicable Privacy Laws, and (ii) where required by Applicable Privacy Laws, for providing adequate notice to and obtaining express and/or adequate consent from individuals so that you and we can lawfully use, process, store and transfer any such Personal Data in accordance with this Agreement. You agree that your indemnity under Clause 10.3 of the Agreement shall include indemnity for any claims alleging a failure or defect in your consents. For the avoidance of doubt, Cepheid and you agree that neither is acting as an advisor, legal or otherwise, to the other.

- (b) we shall ensure that any person we authorize to process Personal Data has committed themselves to keep such Personal Data confidential or are under an appropriate statutory obligation of confidentiality;
- (c) we shall process Personal Data per our **C360 Privacy Policy** at [https://www.cepheid.com/en\\_US/systems/Connectivity/Cepheid-C360](https://www.cepheid.com/en_US/systems/Connectivity/Cepheid-C360) (terms of which may be changed by Cepheid in its sole discretion), the terms of C360 Agreement and our statutory obligations under the Applicable Privacy Laws;
- (d) we shall process such Personal Data on your behalf and in accordance with your lawful documented instructions, and you instruct us to process such Personal Data for the purposes described in Clause 9.2 (subject to Clauses 9.3);
- (e) we shall apply to such Personal Data appropriate technical and organizational security measures as required by Applicable Privacy Laws to protect against unauthorized or unlawful processing, accidental loss or destruction of, or damage to, such Personal Data;
- (f) you consent to our use of Cepheid Service Providers to process Personal Data on your behalf provided that we (i) let you know upon written request the identity and location of the Cepheid Service Providers and their role in the processing of the Personal Data; (ii) impose on the Cepheid Service Providers contractual terms regarding the processing of Personal Data that are at least as robust as the terms set out in this Clause 9.4; (iii) remain liable for ensuring that such Cepheid Service Providers process Personal Data in accordance with this Clause 9.4; and (iv) give you the opportunity to object to a Cepheid Service Provider who processes such Personal Data on reasonable grounds relating to data protection, in which case we may, at our discretion, (A) not appoint or replace the Cepheid Service Provider, if commercially reasonable; or (B) discuss with you in good faith any fees we may require in order to perform our obligations under this C360 Agreement in the absence of such Cepheid Service Provider save that, if the Parties are unable to agree to such fees, or appointment or replacement of the Cepheid Service Provider is commercially not reasonable, then we have the right to give you written notice terminating this C360 Agreement;
- (g) if we transfer Personal Data to another jurisdiction, we shall take reasonable steps to apply an adequate level of protection to the Personal Data. You also acknowledge that the Software may be hosted on servers located outside the country where you are located, and that you have been informed of the server locations. You agree that such hosting, and the export, processing, and storage of Personal Data and User Data outside of the country where such data is collected in connection with Cepheid's performance under this Agreement shall not in and of themselves constitute any breach or violation by Cepheid; and
- (h) for the U.S. customers and C360 Data originating from the United States, the Business Associate Agreement ("**BAA**") attached hereto as Exhibit B shall govern our performance of certain functions, activities, or services for or on behalf of you to the extent they involve the use or disclosure of patient health information as defined in 45 C.F.R. § 160.103. To the extent any provision herein conflicts with a provision of the BAA, the provision herein conflicts with a provision of the BAA, the provision in the BAA shall prevail. This C360 Agreement and the attached BAA shall supersede all earlier versions



of the C360 User Agreements and BAAs between the Customer and Cepheid. For the Canadian customers and C360 Data originating from Canada you and Cepheid are subject to Data Protection Addendum (“DPA”) set forth in Exhibit C hereto in connection with the Personal Data processed by Cepheid under this Agreement, which will apply when and to the extent required by Applicable Privacy Laws, and DPA and its Annexes form an integral part of this Agreement. Where, and to the extent that the DPA applies, if there is any conflict between this Clause 9 and the DPA, the DPA will prevail.

9.5 Upon termination of this C360 Agreement, we shall destroy all Personal Data in our possession or control. This requirement shall not apply (i) to the extent that we are required by applicable law to retain some or all of the Personal Data, or we reasonably believe that such retention is necessary to comply with applicable laws and regulations, or to comply with a legal process or request; (ii) to the extent we reasonably believe that retention of some or all of the Personal Data is appropriate or necessary to take precautions against liability or to protect the rights or safety of us, you, third parties, or the public, (iii) to the extent we reasonably believe that it is appropriate or necessary to detect, prevent or otherwise address security, fraud or technical issues, or (iv) to the extent it is infeasible.

## 10. Liability

10.1 Access to the Software is being provided to you solely for use in accordance with this C360 Agreement. While we will use reasonable skill and care in making the Software available to you, we exclude, to the fullest extent permissible by law, all warranties, representations, conditions or terms which may be implied. Except as expressly provided otherwise in this C360 Agreement, the Software and supporting Documentation are provided to you on an “as is” basis, and we disclaim and do not accept any liability to you or any patients or other third parties in connection with this C360 Agreement. We do not warrant (i) the accuracy or completeness of any data accessed, tracked, collected or otherwise provided to you as part of the Software; or (ii) that the Software is free of bugs, speed issues or performance issues. You acknowledge and agree that the operation of the Software is dependent upon the proper and effective functioning of the Internet, your own and third party equipment and services, your own configuration of the Software functionalities and your own usage of the data made available, and that we do not guarantee and shall not be liable for these in any way for these services. If you transmit or export any of the C360 Data to third-party equipment, you acknowledge and agree that we will not be liable for processing, use, retention or deletion of the transmitted/exported data. This Clause 10.1 is subject to Clause 10.4.

10.2 Neither Party shall be liable to the other for any special, indirect or consequential losses or damages. This Clause 10.2 is subject to Clauses 10.3 and 10.4.

10.3 You are liable for, and shall indemnify and keep us (together with our affiliates, employees, directors, sub-contractors and agents) indemnified from and against any and all claims, demands, proceedings, costs, charges, damages, loss and liability whatsoever incurred or suffered by us whether direct, indirect or consequential (including without limitation any economic loss or other loss of profits, business or goodwill) arising out of any dispute, claims or proceedings brought against us arising out of your use of the Software, Documentation and/or any other Cepheid Confidential Information otherwise than in accordance with the terms of this C360 Agreement and/or your breach of Applicable Privacy Laws.

10.4 No term of this C360 Agreement shall restrict or exclude any liability which by applicable law cannot be so restricted or excluded.

## 11. Confidentiality and Publicity

11.1 Each Party agrees: (i) not to disclose the Confidential Information of the other Party to anyone except its employees, contractors and advisors on a strict need to know basis and subject to a written duty of



confidentiality; (ii) not to use the Confidential Information outside the scope of this C360 Agreement; and (iii) to use all commercially reasonable endeavors to protect the confidentiality of the other Party's Confidential Information, applying at least the same care that it applies to protect its own similar information, but in no event less than reasonable care.

11.2 Clause 11.1 shall not apply to Confidential Information that (i) is or becomes publicly available through no fault of the Recipient, (ii) is already in the Recipient's possession at the time of its disclosure without any duty of confidentiality, or (iii) is independently developed by the Recipient without use of the Discloser's Confidential Information.

11.3 Each Party may disclose Confidential Information of the other Party to the extent required (i) by applicable law or court or governmental order, (ii) to exercise its rights under this C360 Agreement, or (iii) to establish or preserve its rights under this C360 Agreement (collectively "**Compulsory Disclosure**"), provided that a Party who is subject to such a Compulsory Disclosure shall provide prompt prior notice to the other Party as soon as possible of the purported obligation to make such Compulsory Disclosure so that a Party can seek to prevent and/or limit the potential disclosure of its Confidential Information, and provided that if Compulsory Disclosure is required despite a Party's efforts to prevent it, then the disclosing Party shall disclose no more than is legally required and shall make best efforts to maintain the confidentiality of the Confidential Information.

11.4 Notwithstanding Clauses 11.1 and 11.2, we may disclose your Confidential Information to any of Cepheid Service Providers and employees and contractors of our parent and sister companies to the extent necessary to enable us to perform our obligations to you under this C360 Agreement and to perform the activities set forth in this C360 Agreement, including those under Clause 9.2.

11.5 The Parties agree that any actual or threatened breach of this Clause 11 shall constitute immediate, irreparable harm to the innocent Party for which monetary damages would be an inadequate remedy, and that injunctive relief is an appropriate remedy for such breach.

## 12. Miscellaneous Provisions

12.1 **Assignment:** Neither Party may assign, transfer or novate this C360 Agreement or any of its rights and obligations under it, except to a successor, without the express written consent of the other Party.

12.2 **Entire agreement:** This C360 Agreement sets out the entire agreement between you and us and supersedes all previous or contemporaneous understandings, communications, agreements or representations in relation to its subject matter, whether written or oral. If this C360 Agreement is translated into a language other than English and there are conflicts between the translations, to the extent allowed by the applicable law, the English version shall prevail and control. The parties acknowledge and agree that they have required that this C360 Agreement be prepared in the English language. Les parties reconnaissent avoir exigé que les présentes soient rédigées en langue anglaise.

12.3 **Severability:** Any provision of this Agreement that is unenforceable shall be severed and the remaining provisions shall continue in full force and effect.

12.4 **Survival:** Articles/Clauses 1, 3, 4, 6, 8.4, 8.5, and 9 through 12 shall survive termination or expiration of this C360 Agreement.

12.5 **Changes:** Cepheid reserves the right at any time to modify this Agreement and to impose new or additional terms or conditions on your use of the Software. In such case, Cepheid will give you notice of any material adverse change to this Agreement, unless it would not be reasonable to do so due to circumstances arising



from legal, regulatory, or governmental action; to address user security, user privacy, or technical integrity concerns; to avoid service disruptions to other users; or due to a natural disaster, catastrophic event, war, or other similar occurrence outside of Cepheid's reasonable control. In the event that Cepheid does make material adverse changes to the terms of use, you will have the right to terminate this Agreement and your account.

**12.6 Waiver:** Any waiver (which must be in writing) on a particular occasion by either you or us of any rights under this C360 Agreement does not imply that other rights are or will be waived.

**12.7 Force Majeure:** Neither Party shall be in breach of this C360 Agreement or liable for delay in performing, or failure to perform, any of its obligations under this C360 Agreement if such delay or failure results from events, circumstances or causes beyond its reasonable control. In such circumstances the affected Party shall be entitled to a reasonable extension of time for performing such obligations. If the period of delay or non-performance continues for sixty days, the non-delaying Party may terminate this C360 Agreement by giving thirty (30) days' written notice to the delaying Party.

**12.8 Notices:** All notices required to be given to the other Party under this C360 Agreement shall be in writing and shall be sent to the addresses below, or such alternative address as each Party may notify to the other in writing from time to time. Customer has an obligation to keep the addresses listed below up-to-date. Such notices shall be deemed effective upon receipt.

**For Cepheid**

Cepheid  
Attn: Legal/Privacy  
904 Caribbean Drive  
Sunnyvale, CA 94089  
Phone: 408-541-4191  
Email: cepheid.legal@cepheid.com

**For Customer**

Contact information (i.e. Email address(es), mailing address(es), and telephone number(s)) of Customer's Administrator(s) associated with Customer's Software account.

**12.9 No partnership or agency:** Nothing in this C360 Agreement shall be deemed to establish any agency, partnership or joint venture relationship between us and you.

**12.10 Updates.** Cepheid may update the Software from time to time in its sole discretion without notice to you and those updates may be automatically applied to the Software and downloaded or installed onto your device or computer. However, Cepheid will give you notice of any material adverse change to the Software functions such that the updated functions materially change the data collection or modify our data use outlined in this C360 Agreement unless: a change is reasonably necessary to address legal, regulatory, or governmental action; to address your or other users' security, your or other user's privacy, or technical integrity concerns; to avoid service disruptions to other users; or to avoid issues resulting from a natural disaster, a catastrophic event, war, or other similar occurrence outside of Cepheid's reasonable control. In the event that Cepheid does make material adverse changes to the Software, you will have the right to terminate this Agreement and your account.

**12.11 Governing law and jurisdiction:** The laws of the State of California, excluding its conflicts of law provisions, shall govern the validity, construction and effect of this C360 Agreement and the relationship between the Parties. The Parties agree to submit to the personal and exclusive jurisdiction and venue of the courts located within the county of Santa Clara, California, to resolve any dispute or claim arising from this C360 Agreement.

[End of Agreement. Exhibit A, Exhibit B and Exhibit C follow.]

**Exhibit A of Cepheid C360 Terms and Conditions**

**Types of Data Collected by the Software and Their Definitions**

<b>Data Type</b>	<b>Data Sub-categories</b>	<b>Definition</b>
<b>* Analytical Information</b>	Analytical test data	Raw data generated in the course of running a test (e.g. cycle thresholds, raw instrument output, sample type, error code)
	Potentially identifying test data	Time, location, and non-sample/patient identifiers, such as test material and instrument identifiers. (e.g. test timestamps, testing site information, serial numbers, test GUID)
	Cepheid System operator's personal data	Cepheid System operator's personal data (e.g. name, userID)
	Analytical systems data	Data generated by the Cepheid System, including low-level system response data.
<b>Test Result Outcome</b>	Analytical test outcome	Test result value (e.g. positivity/negativity, viral load), excludes invalid tests
<b>Sample ID</b>	Sample ID	Sample identifier used to identify the sample analyzed by the Cepheid System
<b>Authorized User</b>	Authorized User's personal data	(e.g. name, UserID, email, phone number)
<b>Patient information</b>	Patient demographics	Customer's Administrator identified patient demographics such as age, sex, etc.
	Patient ID	Cepheid System operator entered patient identification (e.g. an identification number)

\*Analytical Information is required for base functionality of the Software, including, customer support.



## Exhibit B of Cepheid C360 Terms and Conditions

### **BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“BAA”) is entered into as of the Effective Date of the Cepheid C360 Terms and Conditions, (“C360 Agreement”) to which this document is attached as Exhibit B, by and between the covered entity (“Covered Entity”) and Cepheid (“Business Associate”). Covered Entity and Business Associate collectively are referred to herein as the “Parties.” All capitalized terms not defined in this BAA shall have the meanings set forth in the C360 Agreement.

WHEREAS, the Parties have entered into the C360 Agreement whereby Business Associate performs certain functions, activities, or services for or on behalf of Covered Entity that involve the use or disclosure of Protected Health Information (as defined herein) and Electronic Protected Health Information (as defined herein); and

WHEREAS, this BAA is intended to comply with the requirement for written assurances between the Parties as contemplated by the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E, as may be amended from time to time (the “Privacy Rule”) and the Security Standards for Health Insurance Reform at 45 C.F.R. Parts 160, 162 and 164, as may be amended from time to time (the “Security Rule”); and

WHEREAS, the “Health Information Technology for Economic and Clinical Health” (“HITECH”) Act, contained within the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5, 123 Stat. 226), modifies the Privacy Rule and the Security Rule (hereinafter, all references to the Privacy Rule and the Security Rule shall include all amendments to such rules as may be published from time to time in connection with the HITECH Act, and all references to the HITECH Act shall include any accompanying regulations whether in effect as of the effective date of this BAA or subsequently promulgated); and

NOW, THEREFOR, in consideration of the Parties’ continuing obligations under the C360 Agreement, the agreements herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

#### **1. Definitions**

Except as otherwise defined herein, any and all capitalized terms in this BAA shall have the definitions set forth in the Privacy Rule or the Security Rule.

- (A) “Business Associate” has the meaning set forth above.
- (B) “Breach” has the meaning given to such term in 45 C.F.R. § 164.402.
- (C) “Covered Entity” has the meaning set forth above.
- (D) “Data Use Agreement” has the meaning has the same meaning as the term “data use agreement” in 45 C.F.R. § 164.514(e)(4) of the Privacy Rule. Section 4 of this BAA constitutes a Data Use Agreement.
- (E) “Designated Record Set” has the same meaning as the term “designated record set” in 45 C.F.R. § 164.501 of the Privacy Rule.
- (F) “Electronic Protected Health Information” (“ePHI”) has the same meaning as the term “electronic protected health information” in 45 C.F.R. § 160.103 of the Security Rule, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- (G) “HITECH” Act has the meaning set forth above.



- (H) “HIPAA” means the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191), as amended, together with its implementing regulations.
- (I) “Individual” has the same meaning as the term “individual” in 45 C.F.R. § 160.103 of the Privacy Rule.
- (J) “Limited Data Set” has the same meaning as the term “limited data set” as defined at 45 C.F.R. § 164.514(e)(1).
- (K) “Privacy Rule” has the meaning set forth above.
- (L) “Protected Health Information (“PHI”)” has the same meaning as the term “protected health information” in 45 C.F.R. § 160.103 of the Privacy Rule (including, without limitation, Electronic Protected Health Information), limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- (M) “Required by Law” has the same meaning as the term “required by law” in 45 C.F.R. § 164.103 of the Privacy Rule.
- (N) “Secretary” means the Secretary of the Department of Health and Human Services or his or her designee.
- (O) “Security Incident” has the same meaning as the term “security incident” in 45 C.F.R. § 164.304 of the Security Rule.
- (P) “Security Rule” has the meaning set forth above.
- (Q) “Unsecured PHI” has the meaning given to such phrase in the Breach Notification Rule at 45 C.F.R. § 164.402.

## **2. Obligations and Activities of Business Associate**

- (A) Business Associate acknowledges and agrees that all PHI that is created or received by Covered Entity and used by or disclosed to Business Associate or created or received by Business Associate on Covered Entity’s behalf shall be subject to this BAA.
- (B) Business Associate agrees to not use or disclose PHI other than as permitted or required by this BAA or as Required by Law.
- (C) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this BAA.
- (D) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA, the Privacy Rule or the Security Rule.
- (E) Business Associate agrees to notify Covered Entity promptly following discovery of any Breach of Unsecured PHI. Any notice pursuant to this Section 2(E) will include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate, to have been accessed, acquired or disclosed during such Breach. Business Associate will also provide Covered Entity other available information that Covered Entity is required to include in its notification to the Individual.
- (F) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this BAA or any Security Incident of which it becomes aware.



- (G) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate for, or on behalf of, Covered Entity agrees in writing to substantially similar restrictions and conditions that apply through this BAA to Business Associate with respect to such information.
- (H) Within fifteen (15) days of receiving a written request from Covered Entity, provide to Covered Entity such information as is requested by Covered Entity to permit Covered Entity to respond to a request by an Individual to inspect and obtain a copy of PHI about the Individual that is maintained in a Designated Record Set, for as long as the PHI is maintained in the Designated Record Set, in accordance with 45 C.F.R. § 164.524; to amend PHI or a record about the Individual in a Designated Record Set, for as long as PHI is maintained in the Designated Record Set, in accordance with 45 C.F.R. § 164.526; and for an accounting of the disclosures of the Individual's PHI in accordance with 45 C.F.R. § 164.528.
- (I) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity, available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

### **3. Permitted Uses and Disclosures by Business Associate**

- (A) Except as otherwise limited by this BAA, Business Associate may use or disclose PHI to perform functions, activities or services for or on behalf of Covered Entity as contemplated by the C360 Agreement and any other agreement between the Parties which involves the use or disclosure of PHI, provided that such use or disclosure does not violate the Privacy Rule or the HITECH Act if done by Covered Entity.
- (B) Except as otherwise limited by this BAA, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the present and/or future legal responsibilities of the Business Associate.
- (C) Except as otherwise limited by this BAA, Business Associate may disclose PHI (i) to carry out the present/or future legal responsibilities of the Business Associate or otherwise permitted or required by applicable law, and (ii) when Business Associate is acquired or merged with a third party, in which case, Business Associate reserves the right to transfer the PHI to a successor in interest that assumes Business Associate's obligations under this BAA.
- (D) Except as otherwise limited by this BAA, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any breaches in the confidentiality of the PHI.
- (E) Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).
- (F) Except as otherwise limited by this BAA, Business Associate may use PHI to aggregate data as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), including, without limitation, to create graphic or visual representations of such aggregate data, and use and disclose such aggregated data to others.
- (G) Except as otherwise limited by this BAA, Business Associate may use PHI to create de-identified information sets provided that the de-identification conforms to the requirements of 45 C.F.R. §164.514(b). Once de-identified, data is no longer subject to this BAA.



- (H) Except as otherwise limited by this BAA, Business Associate may use PHI to create a Limited Data Set, and may, pursuant to a Data Use Agreement as set forth in Section 4 between the Parties, use such Limited Data Set for its own research purposes and/or to disclose such Limited Data Set: (i) to other users of Business Associate's Cepheid C360 product, including in the form of graphic or visual representations of such Limited Data Set, for their research, public health activities related, or health care operations, or (ii) solely for the duration of the COVID-19 or other national public health emergency, to the White House Task Force for COVID-19, the Centers for Disease Control and Prevention, and other state and federal government agencies for public health activities related to the COVID-19 pandemic, or any other pandemic when Department of Health & Human Services and/or Office of Civil Rights allow Business Associate to make such disclosure.

#### **4. Data Use Agreement**

Pursuant to Section 3(H) hereof, Covered Entity may receive Limited Data Sets from Business Associate. With respect to any such Limited Data Set, Covered Entity agrees that it will:

- (A) Use or disclose such Limited Data Set only for research, public health activities, health care operations, or as required by law.
- (B) Use reasonable and appropriate physical, technical and administrative safeguards to prevent use or disclosure of the Limited Data Set other than as provided for by this Section 4.
- (C) Report to Business Associate any use or disclosure of a Limited Data Set not provided for in this Section 4 of which Covered Entity becomes aware.
- (D) Ensure that any agent, including any subcontractor, to whom Covered Entity provides the Limited Data Set agrees in writing to the same restrictions and conditions that apply to Covered Entity under this Section 4 with respect to the Limited Data Set.
- (E) Not attempt to identify or contact any of the individuals whose PHI is included in the Limited Data Set.

#### **5. Obligations of Covered Entity on Behalf of Business Associate**

- (A) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation(s) may affect Business Associate's use or disclosure of PHI.
- (B) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- (C) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that it has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

#### **6. Security Rule and HITECH Act Responsibilities of the Business Associate.**

With regard to its use and/or disclosure of ePHI, Business Associate hereby agrees to do the following:

- (A) Comply with 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316, with respect to ePHI, to prevent use or disclosure of ePHI other than as provided for by this BAA.
- (B) Require all of its subcontractors and agents that create, receive, maintain, or transmit ePHI on behalf of the Business Associate to agree, in writing, to adhere to substantially similar restrictions



and conditions (in all material respects) concerning ePHI that apply to Business Associate pursuant to Section 5 of this BAA.

- (C) Report to Covered Entity any Security Incident of which it becomes aware that involves the Confidentiality, Integrity or Availability of the ePHI that it creates, receives, maintains or transmits for or on behalf of Covered Entity. The parties agree that this Section satisfies any reporting required by Business Associate of attempted but Unsuccessful Security Incidents (as defined below) for which the parties agree no additional report shall be required. For purposes of this BAA, "Unsuccessful Security Incidents" include but are not limited to activity such as "pings" and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any other attempts to penetrate such computer networks or systems that do not result in unauthorized access, use or disclosure of ePHI.
- (D) Authorize termination of this BAA by Covered Entity if Covered Entity determines that Business Associate has violated a material term of this BAA, in accordance with Section 6.

## **7. Term and Termination**

- (A) *Term.* The Term of this BAA shall be effective as of the date set forth above, and shall terminate when all the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate for or on behalf of Covered Entity, is destroyed or returned to Covered Entity or, if it is infeasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this Section 7.
- (B) *Termination for Cause.* Upon Covered Entity's or Business Associate's knowledge of a material breach or violation by Business Associate of any provision of this BAA, Covered Entity shall either:
  - (i) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the C360 Agreement and any other agreement between the Parties which involves the use or disclosure of PHI if Business Associate does not cure the breach or end the violation within a reasonable time as specified by Covered Entity;
  - (ii) Immediately terminate the C360 Agreement and any other agreement between the Parties which involves the use or disclosure of PHI if Business Associate has breached or violated a material term of this BAA and cure is not possible; or
  - (iii) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.
- (C) *Effect of Termination.*
  - (i) Except as provided in paragraph (ii) of this Section, upon termination of the C360 Agreement and any other agreement between the Parties which involves the use or disclosure of PHI, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate for or on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. This BAA shall terminate when all such PHI is either destroyed or returned to Covered Entity.
  - (ii) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.



## **8. Notification**

With respect to notice pursuant to paragraph 2(F) above, notice to the Covered Entity shall be made by telephone and followed promptly by a written notice to the contact listed as Customer's Administrator(s) in Customer's Software account. Any other notice to the Covered Entity required or provided for under this BAA shall be made in writing and shall be , mailed by first class mail or sent email to the contact listed as Customer's Administrator(s) in Customer's software account . For notice to the Business Associate: Cepheid, 904 Caribbean Drive, Sunnyvale, CA 94089, Attn: Legal/Privacy Department – BAA, Fax: 408-400-8305, Telephone: 408-548-9190. Either Party may designate a different address in writing to the other.

## **9. Regulatory References**

A reference in this BAA to a section in the Privacy Rule, the Security Rule or the HITECH Act means the section as in effect or as amended.

## **10. Amendment**

The Parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for Covered Entity to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, the Privacy Rule, the Security Rule and the HITECH Act, as amended.

## **11. Survival**

The respective rights and obligations of the Business Associate under Section 7 of this BAA shall survive the termination of this BAA.

## **12. Interpretation**

Any ambiguity in this BAA shall be resolved to permit compliance with the Privacy Rule, the Security Rule and the HITECH Act, as amended. Any conflict between the terms of this BAA and any other agreement relating to the same subject matter, which is the Business Associate requirements under the Privacy Rule, the Security Rule and the HITECH Act, as amended, shall be resolved so that the terms of this BAA supersede and replace the relevant terms of any such other agreement.

## **13. Anti-Assignment**

Neither Party may assign either this BAA or any of its rights, interests or obligations hereunder without the prior written approval of the other Party.

## **14. Severability**

The provisions of this BAA shall be severable, and if any provision of this BAA shall be held or declared to be illegal, invalid or unenforceable, the remainder of this BAA shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

## **15. Governing Law**

Except to the extent that the Privacy Rule, the Security Rule, the HITECH Act, as amended, or other federal law applies, this BAA Agreement and the obligations of the Parties hereunder will be governed by and interpreted in accordance with the laws of the State of California. The Parties agree that each is aware of and is deemed to have been notified of any applicable state or local laws, rules or regulations and each party agrees to comply with such applicable state laws, rules and regulations. The Parties agree that this BAA is hereby deemed to be modified to comply with such applicable state or local laws, rules or regulations.



## EXHIBIT C

### DATA PROTECTION ADDENDUM

This Data Protection Addendum (“**DPA**”) supplements the C360 User Agreement between Customer and Cepheid into which it is incorporated by reference (“**Agreement**”) and contains Annexes 1-2. The terms of the DPA applies when and to the extent they are required by the Applicable Data Protection Law (defined below). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

#### 1. Definitions in the DPA.

- (A) “**Applicable Data Protection Law**” means all data protection and privacy laws and regulations applicable to processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.
- (B) “**Controller**”, “**Processor**”, “**Data Subject**”, “**Personal Data**”, “**Process**”, “**Processing**” and “**Special Categories of Personal Data**” shall have the meanings given in Applicable Data Protection Law.
- (C) “**Customer Personal Data**” means any Personal Data Processed by Cepheid on behalf of Customer pursuant to or in connection with the Agreement.
- (D) “**Cepheid Data**” means any Personal Data in the C360 Data as set out in Exhibit A, Processed by Cepheid as a Controller pursuant to or in connection with the Agreement.
- (E) “**Data Breach**” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure of or access to, Personal Data in C360 Data managed or otherwise controlled by Cepheid.
- (F) “**Services**” means those activities, functions and services that Cepheid performs pursuant to the Agreement.
- (G) “**Sub-Processor**” means any entity or person that Processes Customer Personal Data on behalf of Cepheid in connection with the Agreement.

#### 2. Relationship of the Parties:

2.1 If EU Data Protection Law applies to either Party’s processing of Personal Data under the Agreement, the Parties acknowledge and agree that with regard to the processing of Customer Personal Data, Customer is the Controller and Cepheid is a Processor acting on behalf of Customer as set forth in the Agreement, as further described in **Annex 1** (Data Processing Description) of this DPA. The Parties acknowledge and agree that, with regard to the processing of Customer Personal Data, each Party will comply with the terms set out in Clauses 3 to 7 of this DPA.

2.2 Cepheid shall process Customer Personal Data only (a) in accordance with the Agreement and Annex 1 of the DPA, (b) as otherwise necessary to provide the Services to Customer (which may include investigating security incidents and preventing spam or fraudulent activity, and detecting and preventing network exploits and abuse), (c) as we reasonably believe that it is necessary to comply with applicable law or regulation, (d) as otherwise agreed in writing by the Parties (“**Permitted Processor Purposes**”). Cepheid may make reasonable amendments to Annex 1 by written notice to Customer from time to time as Cepheid reasonably considers necessary to meet the requirements set forth in article 28(3) of the GDPR (and, possibly, equivalent requirements of other Applicable Data Protection Laws).



Nothing in Annex 1 (including as amended pursuant to this section) confers any right or imposes any obligation on any party to this DPA.

2.3 The Parties acknowledge that Cepheid is a Controller of the Cepheid Data and that Cepheid will process the Cepheid Data as a separate and independent Controller strictly for the purposes of described in Clause 9.2(b) and Clause 9.2(c) [to the extent de-identified/pseudonymized Cepheid Data is processed to improve and enhance Cepheid's products/services, or develop new products/services] ("**Permitted Controller Purposes**") and in compliance with the terms set out in Clause 9 of this DPA. In no event will the Parties process Cepheid Data as joint Controllers.

2.4 Each Party shall comply with the obligations that apply to it under the Applicable Data Protection Law.

### 3. Security

3.1 Cepheid shall implement and maintain appropriate technical and organizational security measures that are designed to protect Customer Personal Data from Data Breach and designed to preserve the security and confidentiality of Customer Personal Data at least in accordance with Cepheid's security standards described in **Annex 2**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Cepheid shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR; at a minimum, such measures shall include the measures identified in Annex 2.

3.2 In terms of Cepheid's personnel access to Customer Personal Data, Cepheid shall permit only personnel (employee, agents or contractors) who need to access the relevant Customer Personal Data as reasonably necessary for the purposes of the Agreement, with all such individuals being subject to a duty of confidentiality undertakings or professional or statutory obligations of confidentiality.

3.3 If Cepheid becomes aware of a Data Breach affecting Customer Personal Data, it shall:

- a) provide Customer written notice of the same without undue delay and, where feasible, not later than forty-eight (48) hours after becoming aware of such Data Breach;
- b) provide Customer with timely and sufficient information to meet any obligations to report or inform Data Subjects of the Data Breach under the Applicable Data Protection Laws; and
- c) undertake an investigation of such Data Breach and reasonably cooperate with Customer and take such reasonable steps as directed by Customer to assist in the investigation, mitigation and remediation of such Data Breach.

3.4 Upon request and no more than once per year, we shall:

- (a) subject to the confidentiality terms of the Agreement, permit Customer (with ninety (90) days' notice and at a mutually agreed date during regular business hours) at Customer's own expense to review and inspect Cepheid's policies and records concerning Cepheid's physical and administrative controls related to our processing of Personal Data, or at Cepheid's election, make available to Customer a summary copy of reports by an independent auditor concerning the same; and
- (b) respond to a security questionnaire provided by Customer relating to Cepheid's technical and organizational measures implemented in accordance with Annex 2.

3.5 Upon Customer's reasonable request and with reasonable advance notice, Cepheid shall submit the facilities it uses to Process Personal Data and/or the Personal Data for audit which shall be carried out by



Customer representatives or an auditing body agreed to by both Parties, with the cost associated therewith being borne exclusively by the Customer. Cepheid shall keep appropriate records that support its compliance with its obligations under this DPA and make them available to Customer in connection with any audit referred to in this Section 3.

#### 4. Cooperation with the Customer

- 4.1 Cepheid shall provide reasonable and timely assistance at Customer's expense (including by implementing appropriate technical and organizational measures) for the fulfilment of the Customer's obligations, as reasonably understood by Customer, to respond to (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a Data Subject, supervisory authority or other third party in connection with the Processing of the Personal Data under the Data Protection Laws . If any such request, correspondence, enquiry or complaint is made directly to Cepheid, Cepheid shall promptly inform Customer providing full details of the same. Cepheid shall not respond to such communication directly except as appropriate (for example to direct the Data Subject to contact Customer) or legally required, without Customer's prior authorization. If Cepheid is required to respond to such a request, Cepheid shall promptly notify Customer and provide Customer with a copy of the request unless Cepheid is legally prohibited from doing so.
- 4.2 To the extent required by the Applicable Data Protection Law, Cepheid shall (taking into account the nature of the processing and the information available to Cepheid) provide all reasonably requested information to assist the Customer with any data protection impact assessment or prior consultations with applicable data protection authorities as required by GDPR or equivalent provisions of any other Applicable Data Protection Law.
- 4.3. To the extent required by Applicable Data Protection Law, if Cepheid determines that its processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of an Authorized User or patient, Cepheid shall inform Customer and provide reasonable cooperation to Cepheid (at Customer's expense) in connection with any data protection impact assessment that may be required under the Applicable Data Protection Law.

#### 5. Data Center Locations

Customer acknowledges that Cepheid may transfer and process Customer Personal Data and C360 Data to and in the United States and anywhere else in the world where Cepheid or its Sub-Processors maintain data processing operations. Cepheid shall at all times ensure that such transfers are made in compliance with the requirements of Applicable Data Protection Law.

#### 6. Data Retention and Deletion

Cepheid shall retain Customer Personal Data only for as long as necessary to perform the Services, and at the end of the provision of the Services at Customer's choice delete or return the Personal Data to Customer (unless expressly required otherwise by applicable law, including Applicable Data Protection Law and provide written certification, if requested, to Customer that it has complied with this section.

#### 7. Sub-Processing

- 7.1 Customer authorises Cepheid to appoint Sub-Processors (and permit each Sub-Processor appointed to appoint Sub-Processors) in accordance with this Section 7 and any restrictions in the Agreement.
- 7.2 Customer hereby provides a general consent for Cepheid to use Sub-Processors already engaged as of the date of this DPA provided that Cepheid remains fully liable to Customer for such third party and, in each case as soon as practicable, enters into a written and enforceable agreement with such third party that includes terms that are no less restrictive than the obligations applicable to Cepheid under this DPA.



7.3 If Cepheid is to engage a new Sub-Processor, it will give Customer the opportunity to object to the proposed Sub-Processor. If the Customer objects in writing to the new proposed Sub-Processor within fifteen (15) days after receipt of Cepheid's proposed Sub-Processor (a) Cepheid shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-Processor; or (b) where such a change cannot be made within a reasonable time, notwithstanding anything in the Agreement, Cepheid may terminate the Agreement.

## 8. Controller to Controller Terms

8.1 In relation to any Cepheid Data disclosed to Cepheid for the Permitted Controller Purpose, Customer shall be responsible for complying with all necessary transparency and lawfulness requirements under Applicable Data Protection Law in order to do so, including but not limited to the provision of privacy notices provided by Cepheid to Customer from time to time to Patients and/or Authorized Users and obtaining the Patient's consent to Cepheid's processing activities described in the privacy notices provided (where appropriate).

8.2 Cepheid shall implement appropriate technical and organisational measures to protect Cepheid Data from and against a Data Breach and as set out in Annex 2.

8.3 Cepheid may, at its election, appoint third party Processors to process Cepheid Data for the Permitted Controller Purpose, provided that such processors: (a) agree in writing to process Cepheid Data in accordance with Cepheid's documented instructions; (b) implement appropriate technical and organisational security measures to protect the Cepheid Data against a Data Breach; and (c) otherwise provide sufficient guarantees that they will process the Cepheid Data in a manner that will meet the requirements of Applicable Data Protection Law.

8.4 In the event that either Party receives any correspondence, enquiry or complaint from a Data Subject, regulator or other third party ("**Correspondence**") related to (a) the disclosure of Cepheid Data by Customer to Cepheid for the Permitted Controller Purpose; or (b) the processing of Cepheid Data by the other Party, it shall promptly inform the other Party giving full details of the same, and the Parties shall cooperate reasonably and in good faith in order to respond to the Correspondence in accordance with any requirements under Applicable Data Protection Law.

## 9. Jurisdiction

The Parties submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the law of the country or territory stipulated for this purpose in the Agreement.



## Annex 1 of the DPA Data Processing Description

### **Subject Matter of the Processing**

Cepheid will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by the Customer.

### **Duration of the Processing**

Subject to Section 6 of the DPA, Cepheid will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

### **Processing Operations**

The Personal Data will be subject to the following basic Processing activities (please specify):

Cepheid will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by the Customer, including analysis, generating reports, charts, graphics, investigation, troubleshooting instruments and software, customer support, customer service, and tech support.

### **Data Subjects**

- Patient of Customer
- Authorized Users of Customer authorized by Customer to use the Software and Services

### **Categories of Personal Data**

The Personal Data to be Processed concerns the following categories of data (please specify):

As described in the Agreement and Exhibit A of the Agreement, and any personal data Customer chooses to disclose.

### **Special Categories of Data (if applicable)**

The Personal Data to be Processed concerns the following Special Categories of Data (please specify):

Incidental exposure of Personal Data relating to patient, such as health information, data relating to racial or ethnic origin sex life or sexual orientation, if Customer chooses to disclose.



## **Annex 2 of the DPA**

### **Description of Technical and Organizational Measures Implemented by Cepheid**

- Appropriate technical and organizational security measures to ensure level of security appropriate to the risk.
- Role based access control is implemented.
- C360 Data is encrypted with strong industry standard encryption methods for secure data transfer and storage.
- Multi-tenant database storage securely segregates C360 Data for each Customer and Cepheid uses a separate encryption key for each Customer.
- A mechanism to capture audit trails for user activity is implemented. All users' access to the Software, including Cepheid employees, is controlled with user authentication and authorization. All user actions, including Cepheid employees, within the Software are logged in the audit trail.
- Access to the production servers is limited to authenticated users.
- If additional support is needed outside region, only necessary information will be transmitted, unnecessary Personal Data will be deleted where possible and sent via secure sharing method.
- C360 Data is Processed in secured data centers that are fully managed and monitored 24/7.

End of Exhibit C