Cepheid C360 Privacy Policy

Effective as of October 18, 2021

This Cepheid C360 Privacy Policy (**"Policy"**) sets out how Cepheid, a corporation whose principal place of business is at 904 E. Caribbean Drive, Sunnyvale, CA 94089, U.S.A., including its subsidiaries, which include Cepheid Europe SAS with its principal place of business at Vira Solelh, 81470 Maurens-Scopont, France (**"Cepheid," "we," "us," "our"**) collects and processes personal data about the user (**"Authorized User"**) of our C360 software (**"C360 "**) in the context of an employment or other relationship with the C360 customer **("Institution")** that entered into a Cepheid C360 User Agreement with Cepheid or another agreement that references to C360 Terms and Conditions ("**User Agreement**"), and provides certain information about the rights of Authorized User (**"you," "your"**) and, in certain situations, Institution's patients (**"Patients"**).

In the United States, this Policy does not apply to information about Patients that is protected health information (**"PHI"**) as defined in the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (**"HIPAA"**). Such PHI is protected according to the terms of the HIPAA Business Associate Agreement that accompanies the Cepheid C360 User Agreement entered into between Institution and Cepheid (the **"BAA"**).

Furthermore, this Policy may not apply to research use only products and clinical or other research studies. For collection and processing of personal data in relation to clinical and research studies and the terms of use of C360 for the said studies, please refer to the agreement under which you obtained the relevant Cepheid product.

This Policy aligns with Cepheid's commitment to protecting the privacy and security of the information we collect and process and to being transparent about the ways in which we collect and process your personal data.

1. What is C360?

a. C360 enables Institutions and their Authorized Users to upload data from the compatible and connected Cepheid systems, such as family of GeneXpert systems, including GeneXpert Omni ("**Cepheid Systems**") and/or utilize certain Internet services, including but not limited to, managing data and accessing a real time, aggregated analytics dashboard for the Cepheid Systems and for disease surveillance. It consists of a web portal on Cepheid's hosted infrastructure and a local application or software that runs on computers, hubs or mobile devices provided by Cepheid as part of its Cepheid Systems and enables data gathering and transmission to and from the hosted infrastructure.

b. C360 allows an Institution's administrator to set data collection policies, modify the types of data uploaded and processed, change the level of detail of reports generated by C360 (which may include personal data about Patients), and enable data sharing.

c. C360 requires Internet connectivity, and unless otherwise stated in the agreement under which the Cepheid System was obtained, the Institution is responsible for providing a secure Internet connection and integrating C360 with its existing systems, networks and servers.

2. Patient data processed on C360

a. As noted above, in the United States, this Policy does not apply to PHI as defined under HIPAA. Such PHI is protected according to the terms of the BAA.
b. C360 holds the personal data transmitted or otherwise submitted by Authorized User or Institution in accordance with the data collection policies which the Institution's administrator has set out, information submitted by Authorized Users, and information automatically generated through use of C360 by Authorized User or Institution, but generally such data may include test start time, test end time, test result, cartridge serial number, and a randomly generated identification number that Cepheid cannot link back to a patient name (**"Patient Data"**). In some countries (including, but not limited to France and Canada), such Patient Data provided or included by Institution may be considered personal data, sensitive information or special category of personal data.
c. A controller determines the purposes and means of processing personal data. The controller of Patient Data is your Institution (except for the instances in Section 2(e)) and you may also contact them with any questions about processing of Patient Data or your personal data in relation to C360.
d. A processor processes personal data on behalf of a controller. As a processor, Cepheid processes such Patient Data on behalf of Institutions. Each Institution is primarily responsible for ensuring that the collection and processing of such Patient Data complies with the requirements of applicable privacy and data protection legislation and regulations, including without limitation any applicable requirements concerning the provision of notice to and obtaining adequate consents from Patients where applicable.
e. Cepheid (acting as a processor) will put in place measures to ensure that Patient Data is protected as specified in the User Agreement between Cepheid and the Institution. Cepheid may occasionally act as a controller of the Lab User and Patient personal data for ancillary purposes (e.g. for product improvement and development as set out in Section 3(b) below).
f. Authorized User may include, but is not limited to, epidemiologist user ("**Epidemiologist User**") or end user that operates and uses the Cepheid System connected to C360 ("**Lab User**").
g. If Authorized User receives Patient queries regarding how Institution processes Patient Data on C360, please refer them to the appropriate person within Institution and/or to the Institution's privacy policy.

3. What personal data we collect about Authorized Users and how we use it

a. The personal data we collect on Authorized Users includes data provided by Authorized User or Institution during account registration, and includes information which may personally identify Authorized User, such as Authorized User's name, position, associated Institution and contact details. Authorized User data may also be provided to us when Institution, Authorized User, or Institution's administrator provides such information when using one of the Cepheid Systems in combination with C360. To provide access to C360, we will create a User ID and will provide Authorized User with access details, including a login name and password.
b. We will use Authorized User's data to set up their account, such as Institution's administrator account, Lab User account, or Epidemiologist User account to enable them to access C360 and provide them with support. We also use Lab User's data ("**Lab User Data"**) to monitor and analyze how C360 or other Cepheid products are performing and to create aggregated or pseudonymized statistics and reports to help us improve C360 and other Cepheid products, or develop new products. We may disclose Lab User Data and limited Patient Data, statistics and reports to others and in such circumstances, subject to exceptions set forth in Section 6, will take steps to ensure that we do not disclose data that personally identifies Patients, Lab User or other Authorized Users without their express consent.
c. Our personnel will have access to Authorized User's personal data and Patient Data for the purposes set forth above. Our service, maintenance and support (Tech Support) teams may access Authorized User's data in order to troubleshoot Cepheid System or C360 issues. Tech

Support may access the data collected by the Institution, as well as additional data from the Cepheid Systems such as logs, configuration and certain files for these purposes

4. Patient and Authorized User rights

a. We offer Authorized Users and Patients certain choices in connection with any personal data we may collect about them, including the right to determine how we use their personal data. As noted above, in the United States, this Policy does not apply to PHI as defined under HIPAA. Such PHI is protected according to the terms of the BAA.

b. To the extent provided by applicable law, Authorized Users and Patients may:

i. have the right to access certain personal data we maintain about them and to obtain a copy of their personal data;

ii. update or correct inaccuracies in their personal data;

iii. object (based on legitimate grounds) to our use of their personal data;

iv. block, restrict or delete their personal data from our database;

v. request portability of their personal data;

vi. lodge a complaint with the applicable local privacy authority; and/or

vii. if located in France, they may also (A) provide instructions regarding the manner in which we may continue to store, erase and share their personal data after their death, and where applicable, the person they have designated to exercise these rights after their death, and (B) object-based on legitimate grounds, to the processing of their personal data.

c. Institution or Institution's administrator may access the personal data in Authorized User's online account and correct, amend, or delete personal data at any time.

d. If an Authorized User or a Patient wishes to exercise any of their data protection rights under applicable data protection laws in relation to our processing of Authorized User Data or Patient Data, respectively, the Authorized User or Patient should contact the Institution, which should respond as the controller of the personal data. If an Authorized User or a Patient contacts us to exercise their rights in relation to the personal data that we process as a processor, we will share the request with the Institution and assist the Institution in fulfilling the request in accordance with applicable data protection laws and the terms of our contract with the Institution. Unless otherwise agreed upon by the Institution, we will only respond to a request from Authorized User or a Patient to exercise their data protection rights in relation to their personal data we process as a processor where so instructed by the Institution. We will respond to a request from Authorized User when such request is limited to the Authorized User Data that we process as a controller.

e. When acting as a controller, before we provide Authorized User or Patients with any personal data or correct any inaccuracies, we may ask Authorized User or Patients to verify their identity and to provide other details to help us to respond to Authorized User's or Patient's request. We will endeavor to respond within an appropriate timeframe and, in any event, within any timescales required by law.

f. Where we or the Institution (acting as controllers) rely on consent for us to process Authorized User Data or Patient Data, Authorized User and Patient have the respective right to withdraw their consent at any time.

g. Authorized Users and Patients who wish to exercise their rights under Section 4b(i)-(v) and (vii) above:

i. Patients inquiries should be addressed to the Institution.

Authorized Users may contact Cepheid via email at privacy.officer@cepheid.com, or write to us in the U.S.A at: Cepheid Privacy Officer, 904 Caribbean Drive, Sunnyvale, CA 94089, U.S.A., in Canada at: Canada Privacy Officer, 179 Enterprise Boulevard, Suite 300, Markmam, ON L6G 0E7], or in France at: Cepheid Privacy Officer, Vira Solelh, 81470 Maurens-Scopont, France

5. Legal basis for processing Authorized User / Patient Data

a. If Authorized User is a visitor from the European Economic Area (**"EEA/UK"**) or a Patient in the EEA/UK, our legal basis for collecting and using Authorized User Data as described in Section 3 above will depend on the personal data and the specific context in which we collect it.
b. However, we will normally process personal data only where the Authorized User / Patient has given consent to do so, where we need the personal data to perform a contract with Authorized User or Institution, or to the extent allowed by the applicable law, where the processing is in our legitimate interest and is not overridden by Authorized User's / Patient's data protection interests or fundamental rights and freedoms. For example, we will process Authorized User Data on lawful instructions from Authorized User's Institution in order to fulfill our contract with Authorized User's Institution to provide it with C360, which is in our legitimate interest. For the avoidance of doubt, in Singapore, we will collect, use and disclose personal data only with the Patient's / Authorized User's consent, subject to exceptions under applicable data protection laws.

6. How we share and disclose Authorized User / Patient Data

a. In addition to our personnel, we may share personal data with our parent company, sister companies, and wholly owned subsidiaries listed at https://www.cepheid.com/us/about-us/contact-us and https://www.danaher.com/our-businesses/business-directory, with our secure third party data centers, with support-related service providers located and with additional third parties in the following limited circumstances:
   i. with third party service providers who have a contract with us and help us provide, maintain, support or improve C360 and other Cepheid products;
   ii. with your Institution, including individuals within your organization who are authorized by your Institution to receive your personal data;
   iii. when we have your consent to do so;
   iv. when (i) we are required by law or we reasonably believe that such action is necessary to comply with applicable laws; (ii) we reasonably believe, that such action is appropriate or necessary to take precautions against liability; (iii) we reasonably believe that such action is necessary to protect our, Institution's, Authorized Users', or third parties' rights or security; or (iv) we reasonably believe that it is appropriate or necessary to detect, prevent or otherwise address security, fraud or technical issues. In such circumstances we may disclose your personal data to law enforcement agencies, regulatory organizations, courts or other public authorities; and/or
   v. if we are acquired by or merged with a third-party entity, we reserve the right to transfer or assign the personal data that we hold about you as part of such merger, acquisition, sale, or other change of control.

7. Retention of Authorized User / Patient Data and Aggregated data

a. We will retain personal data only for as long as is necessary to provide C360 to Authorized User or Institution, or (i) to the extent 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 retention is appropriate or necessary to detect, prevent or otherwise address security, fraud or technical issues, (iv) where allowed by the applicable law, to the extent it is infeasible to delete. Institution may remove and/or request our assistance in removing data, including personal data, from C360 at any time unless we are required to retain it by law or regulation. Aggregated data from multiple Institutions, statistics, and reports may be retained in order to provide and improve services, provided that we will never disclose personal data or any data, statistics or reports that identify any identifiable individual without express written consent.

8. Information security

a. All information, including personal data, Authorized User or Institution provide to us is stored on our or our service providers' servers, and we have taken steps to ensure that appropriate technical and organizational measures are applied to protect that information.

b. Communications between C360 and the Authorized User's and/or Institution's Cepheid Systems are encrypted. However, the transmission of any information via the Internet is not completely secure and although we take appropriate steps to protect personal data, we cannot guarantee the security of personal data transmitted to C360 at all times.

c. If Authorized User has a password which enables Authorized User to access their account on C360, Authorized User is responsible for keeping this password secure and confidential.

9. Internet-based transfers

a. C360 is cloud-based software provided as a service to Institutions and their Authorized Users, and as such it requires the transmission of information over the Internet. Given that the Internet is a global environment, using the Internet to collect and process personal data necessarily involves the transmission of data outside the country from which Authorized User is accessing C360 to locations such as Europe and/or the United States of America. We may transfer to, and store the personal data we collect through C360, countries other than the country in which the data was originally collected. Authorized User and Patient acknowledges and understands that (i) we may need to share personal data with our group entities located in countries outside the EEA so that the personal data may be processed for the purposes described above, and (ii) our secure third party C360 cloud servers are located outside of the EEA (as relevant) and may be outside of the country in which you are located, including Canada and the United Kingdom . We will take steps to ensure that personal data continues to be protected and used in accordance with this Policy, including relying on the EU Standard
Contractual Clauses for transfers of personal data between our group entities and third parties as appropriate to provide adequate protection of personal data when it is processed outside the EEA in accordance with European Union data protection laws.

b. Transfer of data outside Nigeria is to be carried out under the supervision of the Honourable Attorney General of the Federation (HAGF) through the issuance of an adequacy decision confirming that the foreign country has data protection laws no less than the level of protection available in Nigeria. Authorized Users and Patients hereby consent to the transfer and storage of their personal data outside Nigeria without an adequacy decision of the HAGF. We will, however, ensure that the personal data is protected in accordance with the standards set out in this Policy.

10. Changes to the Policy

a. This Policy can be updated time to time. By continuing to use C360 after the posting of any changes, Authorized User and Institution confirm Authorized User’s and Institution’s continuing acceptance of this Policy. Institution acknowledges that it is responsible for and will use its discretion to provide Policy updates to its Patients.

11. Additional Notice to Canadian Residents Only

a. In Canada, C360 is provided by Cepheid, who acts as the data controller or processor, as applicable, of personal data pursuant to this Policy.

12. Additional Notice to California Residents Only

Subject to certain limits under California Civil Code § 1798.83, California residents may ask us to provide them with (i) categories of personal data collected, sold or disclosed by us; (ii) purposes for which categories of personal data collected by us are used; (iii) sources of information from which we collect personal data; and (iv) specific pieces of personal data we have collected about you. In

addition, you have the right to opt-out of sale of your personal data. In addition, in some circumstances, you have the right to request deletion of your personal data.

To make this request, California residents may contact us at privacy.officer@cepheid.com or by calling (844) 842-6676.

If you choose to exercise your privacy rights, you have the right to not to receive discriminatory treatment or a lesser degree of service from us.

We do not sell your personal information.

In the last 12 months, we may have disclosed the following personal data with the following category of third parties for the following purpose

Category of personal data	**Categories of sources of collection**	**Business or Commercial Purpose for Use**	**Categories of Third Parties (if any) with whom personal data is shared**
Identifiers of Authorized Users (e.g. names, user names, unique personal identifier, email address, phone numbers, IP addresses)	Directly from you (e.g. forms you complete or information you upload to C360) Automatically generated through your use of Cepheid Systems and C360	Our business purposes, including specifically, performing services under the C360 User Agreement, including maintaining or servicing accounts, providing customer service, verifying customer information, troubleshooting, technical support for Cepheid Systems and products Improving or enhancing our products or develop new products	Internet Service Providers, Data analytics providers, Operating systems and platforms, Affiliates, Vendors and service providers, Third parties integrated into our services, Third parties as required by law and similar disclosures.
Internet or other electronic network activity information,	Login history (e.g. login- time and log-out time; Authorized User activity audit	Performing services under the C360 User Agreement, including	Internet Service Providers, Data analytics providers,

	trail such as creating, viewing, modifying and deleting records in C360)	maintaining or servicing accounts, providing customer service, verifying customer information, troubleshooting, technical support for C360 and Cepheid Systems and products Improving or enhancing our products or develop new products	Operating systems and platforms, Affiliates, Vendors and service providers, Third parties integrated into our services, Third parties as required by law and similar disclosures.

13. Questions about this Policy

a. For questions about this Policy or our handling of personal data:

i. Patients inquiries should be addressed to the Institution.

ii. Authorized User or Institution may contact Cepheid via email at Privacy.Officer@cepheid.com, or write to us in the U.S.A at: Cepheid Privacy Officer, 904 Caribbean Drive, Sunnyvale, CA 94089, U.S.A., in Canada at: Canada Privacy Officer, Canada Privacy Officer, 179 Enterprise Boulevard, Suite 300, Markmam, ON L6G 0E7; in France at: Cepheid Privacy Officer, Vira Solelh, 81470 Maurens-Scopont, France.