Oracle Health Supplier Data Processing Agreement ("OH-SDPA")

Version 07 July 2025

1. Scope, Order of Precedence and Applicability

This Oracle Health Supplier Data Processing Agreement ("**OH-SDPA"**) applies to the Supplier's Processing of Personal Information on behalf of Oracle Health as a Data Processor for its clients and customers (collectively the "Customer"), for the provision of the Services relating to Oracle Health's Customer as specified in the Supplier's Services Agreement or Purchase Order as applicable ("**Services Contract**"). Unless otherwise expressly stated in the Services Contract, this version of the OH-SDPA shall be effective and remain in force for the term of the Services Contract. This OH-SDPA also applies to any future contracted Services which the Supplier provides to Oracle Health and all other activities in which the Supplier comes into contact with, or may come into contact with Personal Information as part of the provision of Services, or when the possibility of this cannot be ruled out.

As used herein, the OH-SDPA and the Services Contract constitutes the parties' "**Agreement**". Other than the addition of the changes below, the terms and conditions of the Services Contract shall remain unchanged and in full force and effect; however, this OH-SDPA shall replace any prior Supplier Data Processing Agreement or other applicable data processing terms between Supplier and Oracle Health under the Services Contract. In the event of a conflict or inconsistencies between (i) the Services Contract or any of the standards and policies referenced in this OH-SDPA such as the OH-SSS or the OSCoE (as identified in Section 3.2 below), and (ii) this OH-SDPA, this OH-SDPA prevails. Capitalized terms not otherwise defined herein have the meaning set out in the Services Contract or Applicable Data Protection Law.

2. Data Processing

Supplier shall ensure that Supplier, and any person Processing Personal Information on Supplier's behalf, shall:

2.1. Process Personal Information only to deliver the Services on Oracle Health's documented instructions in compliance with Applicable Data Protection Law and the Agreement. The Supplier shall not Process Personal Information for any other purpose including for its own commercial benefit.

2.2. Ensure that persons authorized to Process the Personal Information have committed themselves to written data secrecy or confidentiality arrangements in accordance with applicable laws or are under an appropriate statutory obligation of confidentiality. Supplier warrants it has been duly instructed on the protective regulations of such laws. The undertaking of confidentiality shall continue after the termination of this OH-SDPA and the Services Contract.

2.3. (a) Not permit the Processing of Personal Information by any third party (including Supplier's Affiliates) without the express prior written agreement of Oracle Health. If Oracle Health approves Supplier must enter into a written agreement with the Authorized Subprocessor with terms at least as restrictive as this OH-SDPA ("**Terms**"). Supplier shall provide such Terms to Oracle Health promptly upon request, and Oracle Health may share such Terms with its Customers (where required by contract) and/or a supervisory authority competent for Oracle Health or the relevant Customers of Oracle Health ("**Competent Supervisory Authority**"). Supplier remains responsible for all actions by the Authorized Subprocessor with respect to the Processing of Personal Information and shall reasonably assess the Authorized Subprocessor's compliance with its obligations.

(b) Supplier shall either publish on its public website or include as an Exhibit to this OH-SDPA or to each Statement of Work (SOW) to the Services Contract (i) an overview of any Authorized Subprocessors, (ii) the Processing activities subcontracted to such Authorized Subprocessors, and (iii) their locations. Any updates to this list of Authorized Subprocessors must be approved by Oracle Health in writing as set out in 2.3(a) above.

2.4. In the event that Supplier collects Personal Information directly from Data Subjects on behalf of Oracle Health or its Customer, comply with Oracle Health's reasonable instructions to obtain any required consents and provide any required notices to Data Subjects on Oracle Health's or the Customer's behalf.

2.5. Taking into account the nature of Processing, provide reasonable assistance to Oracle Health for the fulfillment of Oracle Health's obligations to respond to Data Subjects' or Oracle Health's requests for exercising Data Subject rights within a reasonable time but at the latest within the time limits prescribed by Applicable Data Protection Law.

2.6. Cooperate and assist Oracle Health or its Customers and take steps reasonably requested to comply with any registration or other obligations applicable to Oracle Health and/or its Customers under Applicable Data Protection Law.

2.7. At Oracle Health's sole discretion, return or delete Personal Information after the termination of the Services Contract or upon Oracle Health's request. The Supplier must certify in writing to Oracle Health, that the return or deletion of Personal Information has been completed in accordance with the Agreement.

3. Security of Processing and Incident Management

3.1. Supplier shall implement and maintain appropriate technical and organizational measures designed to protect Personal Information against any misuse, accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access in compliance with Applicable Data Protection Law, including the use of industry-recognized security standards such as ISO 27001 or similar standards where appropriate.

3.2. In particular, Supplier shall comply with the Oracle Health Supplier Information and Physical Security Standards, including the Oracle Health Technical and Organizational Measures ("**TOMs"**), and any appendices referenced therein ("**OH-SSS**"). The current version is available at https://www.oracle.com/corporate/subcontractors/health-contracts.html. In addition, the Supplier shall comply with the Oracle Supplier Code of Ethics and Business Conduct ("OSCoE") which is available at http://www.oracle.com/corporate/supplier/index.html. Oracle Health may update the OH-SSS or the OSCoE at its discretion to address evolving business risk, security standards and regulatory compliance requirements.

3.3. Supplier shall also:

(a) Keep databases containing Personal Information segregated from other Supplier Personal Information using logical access restrictions;

(b) Log all access to Personal Information, with information identifying the user accessing or seeking access to such Personal Information, when it was accessed (date and time), and whether the access was authorized or denied; and

(c) Maintain audit trails designed to detect and respond to Security Incidents, including logging atypical events (for example, access to Personal Information by unauthorized persons). These audit trails must be maintained at least for one (1) year or the time period prescribed by law, whichever is longer.

3.4. Pursuant to Applicable Data Protection Law and the additional requirements set out in the OH-SSS, Supplier shall implement and maintain appropriate and documented Security Incident procedures and policies designed to (i) detect, analyze, monitor and resolve Security Incidents; and (ii) without undue delay but at the latest within twenty-four (24) hours of any Security Incident, report such Security Incidents to Oracle Health. Such report shall contain a detailed description of the nature of the Security Incident, categories and approximate number of Personal Information records and Data Subjects concerned, name and contact details of a contact point where more information can be obtained, likely consequences of the Security Incident, and measures to address the Security Incident.

4. Documentation and Audit Rights

4.1. Supplier shall maintain readily available information and records regarding the structure and functioning of all systems and processes that Process Personal Information under the Agreement (e.g., inventory of systems and processes). Such information shall include at least a description of (i) Supplier name and contact details, and data protection officer where applicable, (ii) the categories of Processing activities performed on behalf of Oracle Health, (iii) if applicable, the countries to which Transfers occur, (iv) if applicable, the identity of any Authorized Subprocessors and the Processing activities subcontracted to such Authorized Subprocessors, and (v) the technical and organizational measures designed to protect Personal Information against any misuse, accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition, or access.

4.2. Supplier (or its authorized third party auditor) shall regularly audit business processes and procedures that involve the Processing of Personal Information under the Agreement for compliance with the Agreement. A copy of the audit results shall be provided free of charge to Oracle Health upon Oracle Health's request.

4.3. Supplier shall complete a security and privacy assessment questionnaire related to Services, upon Oracle Health's written request. Such a questionnaire may include questions seeking confirmation of compliance with the Agreement and Applicable Data Protection Law. Upon request by Oracle Health, Supplier will also supply a copy of its and its Authorized Subprocessors' most recent third party audit report or attestation, such as an ISO 27001, SOC report, NIST or similar assessment, if Supplier has had such an assessment which may be shared with Oracle Health Affiliates, Customer or any relevant Supervisory Authority. If, after the original security questionnaire assessment, Oracle Health determines that further assessment is warranted, Oracle Health may request, no more than once per year and with thirty (30) days prior written notice, an assessment with a scope to be mutually agreed to related to the Services provided. During such an assessment, Oracle Health may examine Systems related to specific Services performed, to the extent that such review does not compromise Supplier's confidentiality obligations to other clients. Supplier will also ensure that such audits or assessments confirm Authorized Subprocessors' obligations with the terms of the Agreement.

4.4. If relevant to the Agreement with Oracle Health, Supplier shall cooperate and assist with any inquiry or audit by relevant Customers of Oracle Health (or a qualified independent third party auditor selected by such Customer), or a regulatory authority, in the event of a security incident or otherwise required under applicable law.

4.5. In addition, Supplier shall make available to Oracle Health all information necessary to demonstrate compliance with the obligations laid down in this Section, the Terms and any other additional safeguard mechanisms as required under the Applicable Data Protection Law.

4.6. If additional Processing (including Transfer) requirements are necessary for any specific jurisdiction in order for the Processing by Supplier or its Authorized Subprocessors to be compliant with Applicable Data Protection Law, Supplier and Oracle Health shall negotiate in good faith to amend this Agreement to include such requirements and implement these provisions accordingly.

5. Legal Requests, Notifications, Safeguards and Remedies

5.1. Unless expressly prohibited from doing so by applicable law, Supplier shall promptly notify Oracle Health before taking any action and act only upon Oracle Health's instructions concerning: (i) any requests for disclosure of Personal Information by law enforcement, state security bodies or other public authorities ("**Authority**"); (ii) any request by an Authority for information concerning the Processing of Personal Information or other confidential information in connection with the Agreement; and (iii) any complaints or requests received directly from a Data Subject concerning their Personal Information.

5.2. Supplier will, in any case, assess each request for disclosure by an Authority to establish whether it is legally valid and binding on Supplier. Any request that is not legally valid or binding on Supplier will be resisted in accordance with applicable law. Supplier shall in, any case, request the Authority to put the request received on hold for a reasonable delay in order to enable Oracle Health and/or its Customers to contact the Competent Supervisory Authority for an opinion on the validity of the relevant disclosure. If the suspension and/or notification of the request for disclosure is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, Supplier will request the Authority to waive this prohibition and will document that it has made this request. In any event, Supplier will, on Oracle Health's request but at least on an annual basis provide to Oracle Health (which Oracle Health may further share with Customer and possibly a Competent Supervisory Authority) general information on the number and type of requests for disclosure of Personal Information Processed under the Agreement and received in the preceding twelve (12) month period.

5.3. Supplier will promptly inform Oracle Health if it (i) has a reason to believe that it is unable to comply with any of its obligations under the Agreement and it cannot cure this inability to comply within a reasonable time frame; (ii) becomes aware of any circumstances or change in Applicable Data Protection Law, that is likely to prevent it from fulfilling its obligations under the Agreement; or (iii) has reason to believe that any instructions of Oracle Health regarding the Processing of Personal Information would violate Applicable Data Protection Law.

5.4. Supplier shall promptly take adequate steps to remedy any noncompliance with the Agreement and/or Applicable Data Protection Law regarding the Processing of Personal Information by Supplier and any Authorized Subprocessor. Oracle Health will have the right to temporarily restrict or suspend the relevant Processing (or parts thereof) under the Agreement until the noncompliance is remedied. To the extent remediation is not possible or unduly delayed, Oracle Health may terminate the Agreement in whole or in part, without liability or compensation to Supplier being due and without prejudice to other remedies that may be available to Oracle Health under applicable law.

6. Transfers of Personal Information

6.1. **Restricted transfers from EEA and Switzerland.** This Section applies when the Processing of Personal Information by Supplier or its Authorized Subprocessors involves a Transfer from a Member State within EEA or Switzerland to Supplier or its Authorized Subprocessors (i) located outside the EEA or Switzerland and (ii) not covered by an Adequacy Decision.

(a) Where Oracle Health is a Data Processor, such Personal Information may (depending on the relevant Customer agreement) have been Transferred to Oracle Health or an Oracle Health Affiliate outside of EEA or Switzerland under (i) the Oracle BCR-P), or (ii) EU Model Clauses between Oracle Health (and its Affiliates) and the Customer. As the Processing by Supplier and its Authorized Subprocessors may involve Personal Information covered by either of these Transfer Mechanisms, the following applies as applicable:

1. **Oracle BCR-P.** Supplier agrees, and shall ensure that its Authorized Subprocessors agree, that where Supplier or any of its Authorized Subprocessors fails to fulfill their data protection related obligations under the Agreement and an Data Subject has a

claim against Oracle Health or its Customer with respect to such violation, but is unable to enforce the claim against Oracle Health or its Customer, because Oracle Health and/or its Customer have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed their entire legal obligations by contract or by operation of law, the Data Subject can enforce the data protection related obligations of the Agreement against Supplier and/or Authorized Subprocessor as third-party beneficiaries and that the Data Subject may, at his or her choice, submit a claim against Supplier and/or the Authorized Subprocessor to the Competent Supervisory Authority or courts in the country of origin of the data Transfer. The parties agree that in such case the relevant Data Subject shall be entitled to receive compensation for the damage suffered as a result of any breach of the obligations of Supplier and/or its Authorized Subprocessors under the Agreement.

2. **Processor to Processor EU Model Clauses.** Supplier enters into an unmodified set of EU Model Clauses of which the body is incorporated by reference to this Agreement and the Appendices are attached as Module 3 (**Appendix 1 to this OH-SDPA**).

6.2. **Restricted Transfers from the United Kingdom.** When the Processing of Personal Information by Supplier or its Authorized Subprocessors involves a Transfer subject to cross-border transfer restrictions under UK GDPR, from the United Kingdom to Supplier or its Authorized Subprocessors (i) located outside the United Kingdom and (ii) not covered by an Adequacy Decision by the Information Commissioner's Office (ICO), such Transfers are subject to the terms of the EU Model Clauses as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0), or any successor UK Model Clauses which shall be incorporated herein by this reference and will be effective on the date upon which such UK Model Clauses become effective (**Appendix 2 to this OH-SDPA**).

6.3. **Restricted Transfers from Israel.** This section applies to the extent that the Supplier or its Authorized Subprocessor's Processing of Personal Information for Supplier's performance of the Services involves a Transfer from Israel to Supplier or its Authorized Subprocessors ***located outside of Israel*** subject to the Protection of Privacy Regulations (Transfer of Data to Databases Abroad), 5761-200 ("**Transfer Regulations**"). Such Transfers will be governed by the EU Model Clauses of which the body is incorporated by reference to this Agreement and the Appendices are attached as Module 2 **(Appendix 1 to this OH-SDPA)**.

6.4. **Restricted Transfers from Brazil.** This Section applies solely when the Processing of Personal Information by Supplier or its Authorized Subprocessors involves a Transfer subject to cross-border transfer restrictions from Brazil to Supplier or its Authorized Subprocessors (i) located outside Brazil and (ii) not covered by an Adequacy Decision by the Brazil National Data Protection Authority. Such Transfers will be governed by the applicable Brazilian Standard Contractual Clauses as set out in the Agreement.

6.5. **Restricted Transfers Under the Final Rule.** This Section applies solely when Supplier or Supplier Affiliate Accesses Oracle Health or Oracle Health Affiliates' Covered Data. Supplier represents, warrants, and covenants that: (i) neither Supplier nor any Supplier Affiliate who has Access to Covered Data (nor any employee or Subprocessor of Supplier or any Supplier Affiliate who has Access to Covered Data) is a Covered Person; (ii) Supplier and Supplier Affiliates will not engage in any Covered Data Transaction; and (iii) Supplier will immediately notify Oracle Health in writing if any representation in this Section changes or is no longer true.

6.6. **Restricted Transfers from Other Jurisdictions.** In addition to any applicable requirements under Section 7 below, transfers from other jurisdictions globally that have Transfer restrictions are subject to the terms of this OH-SDPA, including any data protection and security policies referenced herein.

6.7. **Additional Safeguards and Remedies.** Oracle Health and Supplier will review any supplemental measures, which may be required based on applicable European Data Protection Law for the transfer

of Personal Information to countries that do not offer an adequate level of protection. Oracle Health and Supplier will work together in good faith to find a mutually acceptable resolution to address such request, including but not limited to reviewing technical documentation for the Services, and discussing additional available technical safeguards and security services.

6.8. **Additional Rights**. Supplier will provide Oracle Health with a copy of the relevant Transfer Mechanism and/or Terms and any other additional safeguard mechanisms as required under the Applicable Data Protection Law promptly upon request. Oracle Health will have the right to terminate the Agreement, in accordance with Section 5.4 above if the approved Transfer Mechanism is invalidated and no alternative approved Transfer Mechanism is put in place or when the related Terms are not adequate or not put into place.

7. Additional Country-Specific Terms

7.1. If the Supplier Processes Protected Health Information ("**PHI**") as defined by the U.S. Health Insurance Portability and Accountability Act ("**HIPAA**"), Supplier shall execute an Oracle Health Business Associate Agreement with Oracle Health and shall implement the applicable safeguards and processes for the handling of PHI that are specified in the HIPAA Privacy and Security Rules.

8. Key Definitions

"**Access** ", "**Country of Concern**", "**Covered Data**", "**Covered Data Transaction**", and "**Covered Person**" have the meanings set out under the Final Rule.

"**Adequacy Decision**" means a decision issued by the European Commission or equivalent Supervisory Authority of other countries where the country has been determined to have an adequate level of data protection under Applicable Data Protection Law.

"**Affiliate**" means, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity.

"**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under the Agreement.

"**Binding Corporate Rules**", "**BCR"**, "**Process**", "**Processing**" and "**Data Processor**", or their equivalent terms have the meanings set out under Applicable Data Protection Law.

"**BCR-P**" means Binding Corporate Rules for Data Processors.

"**Europe**" means the European Economic Area (EEA) and for the purpose of this Agreement, also Switzerland and the United Kingdom (unless otherwise expressly indicated).

"**EU Model Clauses**" means the standard contractual clauses adopted by the European Commission on 04 June 2021 for the transfer of Personal Information from data controllers located in the European Union to data controllers or data processors established outside the European Union or European Economic Area.

"**Final Rule**" means the rule implementing Executive Order 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, along with any additional guidance, advisory opinions, or licensing decisions, issued by the U.S. Department of Justice.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Data Subject**" means an identified or identifiable individual, data subject or similar term as defined under Applicable Data Protection Law and about whom Personal Information may be Processed under the Agreement.

"**Oracle Health**" and "**Supplier**" mean the entities that have executed this OH-SDPA and the Agreement.

"**Personal Information**" means any information recorded in any form relating to a Data Subject or as otherwise defined under Applicable Data Protection Law.

"**Security Incident**" means misappropriation or unauthorized Processing of Personal Information that may affect the confidentiality, security, integrity or availability of the Personal Information.

"**Special Personal Information**" means any of the following types of Personal Information: (i) social security number, taxpayer identification number, passport number, driver's license number or other government-issued identification number; or (ii) credit or debit card details or financial account numbers, with or without any code or password that would permit access to the account; credit history; or (iii) information on race, religion, ethnicity, sex life or sexual orientation, medical or health information, genetic or biometric information, biometric templates, political opinions, religious or philosophical beliefs, political party or trade union membership, background check information, judicial data such as criminal records or information on other judicial or administrative proceedings; (iv) data of children below the age of 16 years; or (v) any other category of Personal Information identified as special or sensitive under Applicable Data Protection Law.

"**Systems**" mean the facilities, systems, procedures, policies and processes used by the Supplier to Process of Personal Information under the Agreement.

"**Transfer**" means the access by, transfer or delivery to, or disclosure of Personal Information to a person, entity or system located in a country or jurisdiction other than the country or jurisdiction from where the Personal Information originated.

"**Transfer Mechanism(s)**" means Binding Corporate Rules, EU Model Clauses and any other transfer mechanism required to undertake a Transfer.

"**UK GDPR**" means the EU General Data Protection Regulation EU/2016/679, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 pursuant to amendments to the EU General Data Protection Regulation EU/2016/679 made by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and 2020, or any successor law or regulation.

Appendix 1
EU Standard Contractual Clauses for Processor to Processor Transfers (Module 3) ("Clauses")

Preamble

1. The unmodified set of the Clauses of which body is incorporated by reference to this Appendix 1 and the annexes are attached as specified under Section 5 below, identified as corresponding to Module 3 in the Implementation Decision adopted by the Commission on June 4th, 2021, applies to the Processing of Personal Information by the Supplier in its role as a Processor as part of the provision of Services under the Agreement between the Supplier and Oracle Health, where such Personal Information is Processed by the Supplier and/or a Supplier Affiliate in a third country outside the EU/EEA that has not received an adequacy finding under Applicable European Data Protection Law.

2. Only to the extent applicable with regards to the Processing of Swiss Personal Information, the Parties wish to clarify that (1) references to EU member states in these Clauses shall not be interpreted in such a way that data subjects in Switzerland are excluded from exercising their rights at their habitual residence in Switzerland, (2) these Clauses also protect data pertaining to legal entities as long as the Swiss Federal Act of 19 June 1992 on Data Protection, as amended, including the Ordinance to the FADP, remains in force; and that (3) the Swiss Regulator is the competent authority for the purposes of the Agreement.

3. The Parties wish to establish additional safeguards for their data transfers outside of the EU/EEA and Switzerland in consideration of the Court of Justice of the European Union Schrems II ruling of 16 July 2020 (Case C-311/18), and therefore the Services Contract describes supplementary measures to address such safeguards.

4. The parties agree to the following modifications in relation to the body of the Clauses:

   a) The parties agree to use option 1 identified under Section 17 of the Clauses and further choose Ireland as governing law for the Clauses.

   b) The parties agree to modify Clause 18 Subsection (b) by adding Ireland as choice of forum and jurisdiction.

5. The following annexes shall be incorporated and considered part of this Appendix 1:

   - Annex I (includes the list of Parties, Description of Transfer, and Competent Supervisory Authority)
   - Annex II - Technical and organisational measures including technical and organisational measures to ensure the security of the data
   - Annex III - List of sub-processors

6. The Clauses apply as of the Effective Date of the Agreement, and will automatically terminate upon the end of the Services Period of the respective Agreement or until replaced by any other Transfer Mechanism, whichever comes first.

7. Only to the extent applicable with regards to the transfers of Personal Information outside of Israel, the Parties wish to clarify that Subject to Section 2.3 of the Agreement, Data Exporter consents to and allows subsequent transfers by the Data Importer to the extent that such transfers are in line with the requirements of the Transfer Regulations.

This Annex has already been completed.

ANNEX I to the Clauses

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: The Oracle Health contracting entity identified in the Services Contract.

Address: The address for the Oracle Health contracting entity identified in the Services Contract.

Contact person's name, position and contact details:

Refer to Section 3 of the Oracle Services Privacy Policy, available at: https://www.oracle.com/legal/privacy/services-privacy-policy.html#1-6

Activities relevant to the data transferred under these Clauses: The Services as defined in the Services Contract or any applicable Statement of Work (SOW).

Signature and date: Signature and date are effective as of the date of the Services Contract.

Role (controller/processor): Processor

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: The Supplier identified in the Services Contract.

Address: The address for the Supplier entity identified in the Services Contract.

Contact person's name, position, and contact details: The Supplier contact details are identified in the Agreement and in the absence, the details are set forth below.

Activities relevant to the data transferred under these Clauses: The Services as defined in the Services Contract or any applicable Statement of Work (SOW).

Signature and date: Signature and date are effective as of the date of Services Contract.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

In-patients and out-patients, medical staff (referring, treating and post-treatment physicians), relatives and contact persons of patients, accompanying persons, staff of rescue and transport services, other employees of hospitals, and health care facilities and their suppliers / sales representatives, representatives and end

users, such as their employees, consultants, contractors, collaborators, partners, suppliers, customers and clients, and other professional experts, and/or other categories as set out in the relevant Agreement.

Categories of personal data transferred
Personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle, medical social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children;; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided, and/or other data as set out in the relevant Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Special Personal Information, including Special Categories of Personal Information, as necessary to perform the services as more fully described in the relevant Agreement and may include medical treatment details including diagnosis, medication, and condition.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).
Throughout the term of the Agreement, personal data may be transferred on a continuous basis.

Nature of the processing
Processing operations are limited to the extent necessary to provide the services as specified under the Agreement.

Purpose(s) of the data transfer and further processing
Data Importer shall solely process personal data for the provision of the services to be provided under the Agreement, and shall not process and use personal data for purposes other than those set forth in the Agreement, as instructed by Data Exporter or as required by law.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.
Personal data will be retained for the duration of the services under the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.
See section on subprocessors in the OH-SDPA.

B. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13
The Irish Data Protection Commission.

ANNEX II to the Clauses

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

As set out in the OH-SSS and TOMs attached thereto. For purposes of the TOMs, any reference to "Cerner" shall mean "Oracle Health".

ANNEX III to the Clauses

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position, and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. Name: …

   Address: …

   Contact person's name, position, and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

3. Name: …

   Address: …

   Contact person's name, position, and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

See section on subprocessors in the OH-SDPA.

Appendix 2

EU Standard Contractual Clauses as supplemented by the UK International Data Transfer Addendum ("UK Clauses") in accordance with the UK GDPR and UK Data Protection Act

Preamble

1. An unmodified set of the Clauses set out in Appendix 1, and supplemented with the UK's International Data Transfer Addendum (version B1.0) (or any successor UK Model Clauses) ("UK Addendum" and collectively, the "UK Clauses"), applies to the Processing of Personal Information by the Supplier in its role as a Processor as part of the provision of Services under the Agreement, between the Supplier and Oracle Health, where such Personal Information is Processed by the Supplier and/or a Supplier Affiliate in a third country outside the United Kingdom that has not received an adequacy finding from the ICO or another competent UK Regulator of Oracle Health acting as a data exporter to the Supplier acting as data importer.

2. The parties wish to clarify that:

   (i) The content required in Tables 1 and 3 of the UK Addendum shall correspond to the respective content in the annexes of the EU Clauses, as supplemented by the Services Contract.

   (ii) The selectable and optional provisions agreed set out in the Preamble to the Clauses shall be mirrored into Table 2 of the UK Addendum.

   (iii) The UK Clauses shall be governed by the laws of England and Wales.

   (iv) The Mandatory Clauses of the UK Addendum shall automatically be incorporated into the Services Contract.

This Addendum does not need to be completed.

Information Commissioner's Office
Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	**Date is effective as of the date of the Services Contract.**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: **The Oracle Health contracting entity identified in the Services Contract.** Trading name (if different): Main address (if a company registered address): **The address for the Oracle Health contracting entity identified in the Services Contract.** Official registration number (if any) (company number or similar identifier): **The official registration number for the Oracle Health contracting entity identified in the Services Contract**	Full legal name: **The Supplier identified in the Services Contract** Trading name (if different): Main address (if a company registered address): **The address for the Supplier identified in the Services Contract** Official registration number (if any) (company number or similar identifier): **The official registration number for the Supplier identified in the Services Contract**
Key Contact	Full Name (optional): **Refer to Section 3 of the Oracle Services Privacy Policy, available at: https://www.oracle.com/legal/privacy/services-privacy-policy.html#1-6**	Full Name (optional): **Unless defined in this OH-SDPA, the Supplier contact details are identified in the Services Contract**

	Job Title: Contact details including email:	Job Title: Contact details including email:
Signature (if required for the purposes of Section (2	**Signature and date are effective as of the date of the Services Contract**	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3	Processor to Processor	X	Not applied	Prior authorization	30 calendar days	
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As described under Annex I to the Clauses included above under this OH-SDPA

Annex 1B: Description of Transfer: As described under Annex I to the Clauses included above under this OH-SDPA

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described under Annex II to the Clauses included above under this OH-SDPA
Annex III: List of Sub processors (Module 3 only): As described under Annex III to the Clauses included above under this OH-SDPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) mean that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except

where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provide greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" mean this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.8(i) of Module 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    e. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard

to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

f. References to Regulation (EU) 2018/1725 are removed;

g. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

h. Clause 13(a) and Part C of Annex I are not used;

i. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

j. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

k. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

l. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

m. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Oracle Health Supplier Data Processing Agreement Addendum for Oracle Israel Ltd. (OH-SDPA)

This addendum applies to Supplier's Processing of Personal Information (as defined in the OH-SDPA) of Oracle's employees, customers and/or partners to provide services for Oracle Israel Ltd. and/or its ultimate parent company Oracle Corporation, and any direct and indirect subsidiaries and affiliates and any successors in interest of Oracle Corporation; within the scope of the Protection of Privacy Law, 1981 and regulations enacted thereunder, including without limitations, the Protection of Privacy Regulations (Data Security) 2017, guidelines issued by the Israeli Protection of Privacy Authority, and in particular Guideline No. 2/2011 regarding the use of outsourcing for processing Personal Information, as well as any law, regulation and/or administrative directive that apply to Oracle or the Supplier in connection with the processing of the Personal Information (collectively the "**PPL**"). This addendum supplements the terms of Oracle OH-SDPA and the terms here should be read in conjuction with the terms of OH-SDPA. In the event of any contradiction between the terms of the OH-SDPA and the terms of this addendum, then the terms of this addendum shall prevail. The Supplier hereby agrees to the following:

(a) During the service period of the agreement, the Supplier may have access to database systems that are subject to a high security level. The Supplier undertakes to comply with any applicable requirements of the PPL related to these databases and with any additional data security instructions set by Oracle to comply with such requirements.

(b) At Oracle's sole discretion, to return or delete Personal Information pursuant to the Oracle Supplier Information and Physical Security Standards upon completion of the Services or after the termination of the Services Contract or upon Oracle's request, and confirm such return or deletion to Oracle.

(c) To comply with the applicable requirements of the PPL and with any additional data security instructions set by Oracle in order to comply with such requirements.

(d) To ensure that its authorized users sign an undertaking to protect the confidentiality of the Personal Information, to use the Personal Information only according to the Services Agreement and to implement the data security measures prescribed in the OH-SDPA and any accompanying documents.

(e) To report, at least annually, on the manner the obligations under the OH-SDPA and all accompanying documents are implemented by it.

(f) Without derogating from the Supplier's responsibility under the OH-SDPA and any accompanying documents (or any other agreement between the parties, including the Services Contract) and under any law, and notwithstanding any other provision in any other agreement between the parties (including the Services Agreement), the Supplier shall purchase and maintain throughout the term of the OH-SDPA or the term in which it retains the Personal Information, insurance coverage such as a professional liability insurance and/or cyber security insurance which is customary and sufficient to cover the liability of the Supplier for breaches of its obligations and duties under the OH-SDPA and all accompanying documents.

(g) The Supplier shall promptly report Security Incidents to Oracle. In addition, to the extent the Personal Information processed by the Supplier is from a database with a medium security level, Supplier shall hold a discussion with respect to Security Incidents analyzed by it and their implications (including with respect to the requirement to update the security policies) at least on an annual basis, and if such database is of a high security level, on a quarterly basis.

(h) To appoint a data security officer and/or a data protection officer, if required under the PPL and in accordance with the PPL's provisions, and to ensure that such officers perform their obligations under the PPL.

(i) The information security policies of the Supplier shall include provisions regarding all aspects required to be included in such procedures under the PPL (including in light of the security level of the databases which Supplier processes personal information from). The security policies will be updated from time to time as and if required, including due to applicable developments in technology risks or material changes in the systems on which or from which Personal Information is processed or changes in the processing procedures. A review of the necessity of such updates will be performed at least on an annual basis. Supplier will provide the applicable details of the security policies to those acting on its behalf to the extent necessary for the purpose of performing their roles.

(j) To maintain an up-to-date document of the structure of the Supplier's computing systems that will contain or store the Personal Information and/or from which the Personal Information may be accessed, as well as an up-to-date inventory of such systems, including: (a) hardware infrastructure, types of information components and information security; (b) software systems used for operating, managing, maintaining, monitoring, supporting and securing such systems and other data system used by the Supplier, including programs and interfaces used to communicate with and from such systems; and (c) a diagram of the network in which such systems operate (including a description of the connections between the different system components and their physical location). The structure document and inventory will be updated by the Supplier as necessary. The up-to-date structure document and inventory shall only be provided to those acting on behalf of Supplier to the extent necessary for the purpose of performance of their roles.

(k) To the extent the Personal Information processed by the Supplier is from a database with the high security level, the Supplier shall, at least once every 18 months: (1) perform a survey to identify information security risks, review the results of the survey and examine the need to update the security policies accordingly and correct the deficiencies that were discovered as part of the risk survey, if any; and (2) conduct penetration tests for the Supplier's systems to examine their resistance to internal and external risks, review the results of the tests and to act to correct the deficiencies that were discovered.

(l) To perform security awareness training berfore personnel receive access to Personal Data or systems from which such Data may be accessed and when the scope of their access changes.

(m) To the extent the Personal Information processed by the Supplier is from a database with the medium or high security level, the identification manner with respect to access to Personal Information will be, as much as possible, by a physical mean subject to the exclusive control of the person authorized to access the Personal Information.

(n) To maintain all logs/audit trails collected in accordance with the requirements under the OH-SDPA and the accompanying documents and the requirements under the PPL for a period of at least 24 months and to notify anyone who received access to the Personal Information or to the systems in which it is processed or accessed from, of the existence of such logs/audit trail.

(o) To the extent the Personal Information processed by the Supplier is from a database with the medium or high security level, to perform internal or external audit by an auditor with the appropriate skills for performing data security audits, in order to ensure compliance with the OH-SDPA and accompanying documents and the PPL. Such audit will take place at least once every 24 months and it shall not be performed by Supplier's CISO (in the event of an internal audit). Supplier will implement appropriate measures required to remedy any faults or gaps identified during such audit, without undue delay. In the event that Supplier upholds the requirement to perform risk surveys in accordance with Section (m) above, then Supplier will may comply with this obligation within the framework of such risk survey.

(p) To retain logs/audit trails and all security documentation data generated as a result of the implementation of all measures under the OH-SDPA and any accompanying documents and the PPL

by Supplier, for the period required under the PPL. In addition, Supplier shall back up such logs/audit trails and security documentation data in a manner ensuring that such files can be restored to their original form at all times.

(q) To the extent the Personal Information processed by the Supplier is from a database with the medium or high security level, Supplier will determine as part of its security polices a procedure for performing a backup as stated in section (r) above in a periodic and routine manner and a procedure for ensuring the restoration of the aforementioned data. In addition, as part of the documentation of security incidents, the procedures for restoring the information will also be documented, including the identity of the person who performed the restoration procedures and the details of the restored information (the "Restoration Procedures"). To the extent that such database is subject to the high security level, Supplier will be responsible for retaining the backup copy of the aforementioned data and the Restoration Procedures, in a way that ensures the integrity of the information and the possibility of restoring the information in the event of loss or destruction.