Data Processing Addendum ("**Agreement**")

Last updated 11 Feb. 2025

BETWEEN

(1)

Mirion Medical GmbH	Landsberger Strasse 318, 80687, München, Germany
Mirion Technologies (Capintec), Inc.	7 Vreeland Road, Florham Park, NJ 07932 USA
Mirion Technologies (Dosimetry Services) B.V.	Utrechtseweg 310 – B54, 6812 AR Arnhem The Netherlands
Mirion Technologies (GDS), Inc.	104 Union Valley Road, Oak Ridge, TN 37830, USA
Sun Nuclear B.V.	Poolseweg 36, 4818 CG Breda, The Netherlands
Sun Nuclear Corp.	3275 Suntree Blvd., Melbourne, FL 32940, USA
Sun Nuclear GmbH	Landsberger Strasse 318, 80687, München, Germany

(hereinafter individually and collectively referred to as "Mirion Medical")

and

(2) The legal entity that is party to and executed the underlying Services Agreement as a Customer or the underlying Distributor Agreement as a Distributor (the "**Customer**").

BACKGROUND

(A) Mirion Medical provides services ("**Services**") to the Customer pursuant to an agreement ("**Services Agreement**"). Such services may include, without limitation, dosimetry services and radiotherapy quality assurance, as well as support, maintenance, repair and training related to all products and software (both installed on Customer's premises or provided as SaaS) of Mirion Medical.

(B) This Agreement forms part of and is incorporated by reference into the Services Agreement entered into by the Customer and Mirion Medical concerning Customer's use of the Services to reflect the parties' agreement regarding the Processing of Personal Data in accordance with Data Protection Legislation and sets out the framework for the transferring of Personal Data from the Customer to Mirion Medical to be processed for the purpose of providing the Services.

(C) The legal entity or entities of Mirion Medical that are a party or parties to the Services Agreement are also party or parties to the present Agreement with Customer.

(D) This Agreement consists of the terms described herein, Schedule 1, Schedule 2 and Schedule 3 including any Attachments thereto. By executing the Services Agreement, the parties are agreeing to all parts of this Agreement.

1 Definitions

1.1 In this Agreement

1.1.1 "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity; "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly;

1.1.2 "**Customer Personal Data**" means any Customer Data that is Personal Data that Mirion Medical processes on behalf of Customer in the course of providing the Services;

1.1.3 "**Data Protection Legislation**" shall mean one or more of the following as may be applicable to the Personal Data Processed by Mirion Medical on behalf of the Customer in its provision of the Services: (i) General Data Protection Regulation ("**GDPR**") meaning (a) where applicable the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"), or (b) where applicable the EU GDPR as implemented into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), (ii) Data Protection Act 2018 (UK), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), and (iv) Act on the Protection of Personal Information (Act no. 57 of 2003, as amended; "**APPI**"), and

in each case shall include any equivalent legislation in such jurisdictions which shall apply to Processing of Personal Data, in each case as amended, extended or re-enacted from time to time and all orders, regulations, statutes, instruments or other subordinate legislation made thereunder the European Union ("**EU**"), the European Economic Area ("**EEA**") and their member states, Switzerland the United Kingdom ("**UK**") and in Japan from time to time;

1.1.4 "**Data Subject**", "**Controller**", "**International Organization**", "**Processor**", **"Business Operator",** and "**Processing**" have the same meaning as in the Data Protection Legislation, or the equivalent meaning if the Data Protection Legislation does not use or refer to the exact same concept;

1.1.5 "**Personal Data**" has the meaning set out in the Data Protection Legislation;

1.1.6 "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy decision by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018, (iii) where the FADP applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of states with an adequate level of data protection published in Annex I of the Swiss Data Protection Ordinance, and (iv) where the APPI applies, a transfer of personal data outside Japan, except to a country named in a decision of adequacy adopted pursuant to Article 28.1 of the APPI;

1.1.7 "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the standard contractual clauses adopted by the European Commission by Commission Implementing Decision (EU) 2021/914 for the transfer of personal data to third countries pursuant to the EU GDPR ("**EU Standard Contractual Clauses**" or "**EU SCCs**"), (ii) where the UK GDPR applies, (a) for so long as it is lawfully permitted the standard contractual clauses for the transfer of personal data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 adopted pursuant to or permitted under Article 46 of the UK GDPR ("Prior UK SCCs"); and (b) where sub-clause 1.1.7 (ii)(a) does not apply, and

the respective parties are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a UK Addendum, the EU SCCs, subject to the execution of the UK Addendum amended as specified in Schedule 3, and (iii) where the FADP applies the EU SCCs.

1.1.8 "**Sub-processor**" means any third party (including any Mirion Medical Affiliates) engaged by Mirion Medical to process any Customer Personal Data (but shall not include Mirion Medical employees or consultants);

1.1.9 "**Third Country**" means (i) where the EU GDPR applies, a country outside of the European Economic Area, which is not subject to an adequacy decision by the European Commission; (ii) where the UK GDPR applies, any country other than the UK, which is not subject to an adequacy finding by the Information Commissioner's Office ("**ICO**"), (iii) where the FADP applies country outside of Switzerland which is not included on the list of states with an adequate level of data protection published in Annex I of the Swiss Data Protection Ordinance, and (iv) where the APPI applies, any country other than those subject to a decision of adequacy adopted pursuant to Article 28.1 of the APPI;

1.1.10 **"UK Addendum"** means the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, as such Addendum may be revised under Section 18 therein.

2 Data Processing

2.1 For the purposes of the Data Protection Legislation, Mirion Medical is a Processor or Sub-Processor acting on behalf of the Customer, who is the Controller, Processor or Business Operator the Personal Data. Where Customer processes the Data as a Processor on behalf of its own customers and Mirion Medical acts as a Sub-Processor, Customer warrants that the instructions given to Mirion Medical will be in accordance with the instructions to Customer by its own customers and, where the APPI shall apply, warrants that the instructions given to Mirion Medical will be in accordance with the Personal Data usage notified to the Data Subjects.

2.2 The nature, purpose and duration of the Processing, the categories of Personal Data and the categories of Data Subjects whose Personal Data is being Processed in connection with the

Services are set out in Schedule 1 of this Agreement. In addition to the obligations stipulated herein, each Party shall comply with its obligations under applicable Data Protection Legislation in respect of any Personal Data it processes under the Agreement.

2.3 Customer will serve as the sole point of contact for Mirion Medical with regard to any third-party Controllers of the Customer Personal Data. Mirion Medical need not interact directly with (including seek any authorizations directly from) any such third-party Controllers (other than through regular provision of the Services to the extent required by the Services Agreement). Where Mirion Medical would (including for the purposes of the EU SCCs) otherwise be required to provide information, assistance, cooperation, or anything else to such third-party controllers, Mirion Medical may provide it solely to Customer. Notwithstanding the foregoing, Mirion Medical is entitled to follow the instructions of such third party with respect to such third party's Customer Personal Data instead of Customer's instructions if Mirion Medical reasonably believes this is legally required under the circumstances; and, where the APPI applies, Mirion Medical shall inform Customer reasonably in advance.

2.4 Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired Customer Personal Data. Customer represents and warrants that:

2.4.1 it has provided, and will continue to provide, all notices and obtained, and will continue to obtain, all consents, permissions and rights necessary under Data Protection Legislation for Mirion Medical to lawfully process Customer Personal Data on Customer's behalf and in accordance with its instructions;

2.4.2 it has complied with all applicable Data Protection Legislation in the collection of and provision to Mirion Medical and its Sub-processors of such Customer Personal Data; and

2.4.3 it will ensure its Processing instructions to comply with applicable laws (including Data Protection Legislation) and that the processing of Customer Personal Data by Mirion Medical in accordance with the Customer's instructions will not cause Mirion Medical to be in breach of applicable Data Protection Legislation.

2.5 Mirion Medical shall comply with its obligations under the Data Protection Legislation and shall:

2.5.1 process the Personal Data only to the extent necessary for the purpose of providing the Services and in accordance with the Customer's written instructions (including with respect to transfers of Personal Data to a Third Country or to an International Organization);

2.5.2 implement appropriate technical and organizational measures in accordance with the Data Protection Legislation to ensure a level of security appropriate to the risks that are presented by such Processing, in particular, from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing and the likelihood and severity of risk in relation to the rights and freedoms of the Data Subjects as set out in Schedule 2;

2.5.3 ensure that any employees or other persons authorized to Process the Personal Data are subject to appropriate obligations of confidentiality and understand Mirion Medical's obligations of security with regard to the Personal Data;

2.5.4 on request by the Customer and taking into account the nature of the Processing and the information available to Mirion Medical, reasonably assist Customer in ensuring compliance with its obligations under the Data Protection Legislation in respect of the Personal Data processed by Mirion Medical on behalf of Customer for the purpose of providing the Services;

2.5.5 engage any third-party Sub-processor to carry out its Processing obligations under this Agreement by way of a written contract so that such third party will, at all times during the engagement, be subject to data protection obligations at least equivalent to those set out in this Agreement;

2.5.6 notify the Customer, as soon as reasonably practicable, about any request or complaint received from a Data Subject (without responding to that request, unless authorized to do so by the Customer) and reasonably assist the Customer by technical and organizational measures, insofar as possible, for the fulfilment of the Customer’s obligations in respect of such requests and complaints;

2.5.7 notify the Customer as soon as reasonably practicable on becoming aware of a Personal Data breach and cooperate with Customer to allow Customer to meet

its reporting obligations in case of a Personal Data Breach;

2.5.8 where the APPI applies, in case of leak or unauthorized disclosure of Personal Data ("Leak"), the Parties shall immediately consult together on the measures to adopt to stop or mitigate the Leak and to prevent a repeat of the Leak. The Parties shall investigate the reasons that made the Leak possible and shall allocate the responsibility for the Leak among themselves based on the results of said investigation. Any damages due to third parties by reason of the Leak shall be similarly borne by each Party in proportion to its responsibility for the Leak;

2.5.9 where the APPI applies, inform Customer of any changes to the Data Protection Legislation applicable to Mirion Medical if and to the extent that it may impact the performance of Mirion Medical's obligations under this Agreement;

2.5.10 where the APPI applies, report to Customer at Customer's request on the status of Mirion Medical's performance of its obligations hereunder;

2.5.11 notify the Customer, unless prohibited from doing so under Data Protection Legislation, if it becomes aware that any data processing instruction from the Customer violates Data Protection Legislation or if it is unable to comply with the Customer's data processing instructions, in which case, the Customer is entitled to withdraw or modify their processing instructions;

2.5.12 on request by the Customer and to the extent reasonably possible, make available information necessary to demonstrate the Customer's compliance obligations under the Data Protection Legislation and on reasonable advance notice in writing permit, and contribute to, audits of compliance with Data Protection Legislation and this Agreement carried out by the Customer (or its authorized representative);

2.5.13 on termination or expiry of this Agreement, destroy, delete or return (as the Customer directs) all Personal Data and delete all existing copies of such data unless required by law to keep or store such Personal Data.

2.6 The Customer consents to the engagement of Sub-processors. This authorization will constitute Customer's prior written consent to the subcontracting by Mirion Medical of the Processing of Personal Data as required under the Standard Contractual Clauses or the Data Protection Legislation.

2.7 Mirion Medical may, from time to time, engage new Sub-processors. Mirion Medical will give Customer notice of any new Sub-processor at least 30 days in advance of providing that sub-processor with access to Customer Data by updating the website and providing the Customer notice of that update. Said notice shall indicate the Data Protection Legislation applicable to said Sub-processor. The Customer may object to Mirion Medical's use of a new Sub-processor by notifying Mirion Medical in writing within ten 10 business days after receipt of Mirion Medical's notice. If the Customer does not approve of a new Sub-processor, then the Customer may terminate the applicable Agreement(s) without liability with respect only to those Services that cannot be provided by Mirion Medical without the use of the objected-to new Sub-processor by providing, before the end of the relevant notice period, written notice of termination.

2.8 The Customer acknowledges that clause 2.5.1 shall not apply to the extent that Mirion Medical is required by law to Process the Personal Data other than in accordance with the Customer's instructions and Mirion Medical acknowledges that, in such a case, it must promptly inform the Customer of the relevant legal requirement prior to Processing unless the law prohibits the provision of such information.

2.9 The Customer is responsible for reviewing the information made available by Mirion Medical relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under the applicable Data Protection Legislation. Customer acknowledges that the technical and organizational measures described in Schedule 2 are subject to technical progress and development and that Mirion Medical may update or modify these technical and organizational measures from time to time provided that such updates and modifications do not result in a material degradation of the overall security of the Services subscribed to by the Customer. Where the APPI applies, Mirion Medical shall further cooperate with Customer's reasonable requests of improvements or changes to the technical and organizational measures, subject to either Party having the right to terminate this Agreement should said improvements or changes not being possible for Mirion Medical.

2.10 If Mirion Medical becomes aware that any law enforcement, regulatory, judicial or governmental authority (an "**Authority**") wishes to obtain access to or a copy of some or all Customer Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Personal Data to such Authority, Mirion Medical shall:

2.10.1 immediately notify Customer of such Authority's data access request;

2.10.2 inform the Authority that it is a Processor of Customer Personal Data and that Customer has not authorized it to disclose that Personal Data to the Authority;

2.10.3 inform the Authority that any and all requests or demands for access to Customer Personal Data should be notified to or served upon Customer in writing; and

2.10.4 not provide the Authority with access to Customer Personal Data unless and until authorized by Customer.

2.11 In the event Mirion Medical is under a legal prohibition or a mandatory legal compulsion that prevents it from complying with clause 2.10 in full, Mirion Medical shall use reasonable and lawful efforts to challenge such prohibition or compulsion, while Customer acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended Authority access request.

2.12 If Mirion Medical makes a disclosure of Customer Personal Data to an Authority (whether with Customer's authorization or due to a mandatory legal compulsion) Mirion Medical shall only disclose Customer Personal Data to the extent Mirion Medical is legally required to do so and in accordance with applicable lawful process and shall, to the extent legally possible, inform Customer of the nature and scope of the Customer Personal Data disclosed.

2.13 Clauses 2.10 to 2.12 shall not apply in the event that, taking into account the nature, scope, context and purposes of the intended Authority's access to the Customer Personal Data, Mirion Medical has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual. In such event, Mirion Medical shall notify Customer as soon as possible following such Authority's access and provide Customer with full details of the same, unless and to the extent Mirion Medical is legally prohibited from doing so.

2.14 Mirion Medical shall not knowingly disclose Customer Personal Data to any third party unless authorized under this Agreement.

2.15 Mirion Medical shall have in place and maintain in accordance with good industry practice measures to protect Personal Data from interception (including in transit from Customer to Mirion Medical and between different systems and services). This includes having in place and maintaining network protection to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit to deny attackers the ability to read data.

2.16 Each Party shall designate a representative in charge of coordinating with the other Party the performance of each Party's obligations hereunder.

3 Data Transfers

3.1 Personal data that Mirion Medical Processes under the Agreement may be Processed in any country in which Mirion Medical, its Affiliates and authorized Sub-processors maintain facilities to perform the Services. Mirion Medical shall not Process or transfer Customer Personal Data (nor permit such data to be Processed or transferred) outside of the EEA, Switzerland, the UK, or Japan unless it first takes such measures as are necessary to ensure the transfer is in compliance with this Agreement and applicable Data Protection Legislation. The countries in which the Processing shall take place shall only be those identified in Schedule 1 as amended from time to time by the Parties.

3.2 The Parties agree that when the transfer of personal data from Customer (as "data exporter") to Mirion Medical (as "data importer") is a Restricted Transfer and Data Protection Legislation requires that appropriate safeguards are put in place, such transfer shall be subject to the Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA as set out in Schedule 3. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Services Agreement or this Agreement the Standard Contractual Clauses shall prevail to the extent of such conflict.

3.3 If Mirion Medical adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to applicable Data Protection Legislation) for the transfer of personal data not described in this Agreement ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this Agreement (but only to the extent such Alternative Transfer Mechanism complies with applicable Data Protection Legislation and extends to the territories to which the relevant personal data is transferred).

4 General

This Agreement shall be governed by the law of France.

Schedule 1

Data Processing

List of parties	
Controller or Processor / Data exporter	Customer
Processor or Sub-Processor / Data Importer	For dosimetry services: Mirion Technologies (Dosimetry Services), B.V., NL, Mirion Medical GmbH, DE, and/or Mirion Technologies (GDS), Inc., US. Contact person: Edwin Ulbricht, email: privacy@mirion.com. For radiotherapy quality assurance (products, SW and related services): Sun Nuclear B.V., NL, Sun Nuclear Corp., US, and or Sun Nuclear GmbH. Contact person: Fernando Otero, email: privacy@mirion.com. For all other cases: The Mirion Medical entity or entities that are a party to the Services Agreement. Contact: privacy@mirion.com.
Description of the processing / transfer	
Nature/purpose of Processing	Dosimetry services: Customer personal data are processed to measure, track, keep record of and report to Customer on exposure to ionizing radiation for occupational and other radiation safety purposes. Radiotherapy quality assurance (products, SW and related services): Customer personal data are processed to ascertain that radiotherapeutic treatment is performed as specified by competent medical personal. The data are further processed to maintain, repair, configure and/or customize products and SW provided by Mirion Medical as well as for training of Customer personnel. Other cases: Customer personal data are processed to provide the Services according to the Services Agreement.

<table>
<tr><td>Categories of Data Subjects</td><td colspan="3">For all cases, categories of data subjects may include one, several or all of the following categories:
- employees of the data exporter,
- employees of the data exporter’s customers,
- patients under treatment by the data exporter,
- patients under treatment by the data exporter’s customers.</td></tr>
<tr><td>Categories of Personal Data</td><td>Dosimetry services:
• Full name
• Gender
• Identification numbers as required by applicable regulations
• Date of birth
• Occupation, employer
• Occupational/Industry category
• Start date and end date of monitoring
• Professional email address
• Professional address
• Home address</td><td>Radiotherapy QA by means of SunCHECK (SaaS):
SunCHECK Patient and SunCHECK Machine:
• Staff (medical physicist) full name (surname, first name(s), initial(s))
• Staff (medical physicist) email address
SUNCHECK Patient
• Patient full name (surname, first name(s), initial(s))
• Patient date of birth
• Patient gender</td><td>Other cases:
• Full name
• Professional function/role
• Professional email address
• Professional address
• Professional phone numbers</td></tr>
<tr><td>Special Categories of Personal Data or Personal Data requiring special consideration</td><td>Dosimetry services:
• Radiation dose.
• In addition, the personal data may – but do not necessarily – include the pregnancy start and end dates of the data subject.</td><td>Radiotherapy QA by means of SunCHECK (SaaS):
SUNCHECK Patient
• Patient full name (surname, first name(s), initial(s))
• Patient date of birth
• Patient gender
• Medical Record Number
• Patient global unique identifier within SunCHECK
• SunCHECK user defined name for treatment plan
• Date treatment plan was last modified
• User defined name identifying treatment machine to be used for treatment delivery
• User defined location of intended treatment
• User defined prescription dose for treatment plan
• Total number of fractions for treatment plan
• Treatment modality (3D, CRT, IMR, VMAT, Brachytherapy, SRS Cones, Electron, or Other)
• Additional user-supplied treatment detail
• Global defined name for treatment plan within SunCHECK</td><td>Other cases:
None.</td></tr>
</table>

Third Countries or International Organizations Personal Data will be transferred to	All cases: United States of America
Frequency of the Transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Method of Transfer where the APPI applies	Electronic transmission
Duration of the Processing:	For the term of the underlying Services Agreement until deletion of the Personal Data by Mirion Medical in accordance with the Services Agreement and/or applicable law.
Period for which the Personal Data will be retained, or if that is not possible the criteria used to determinate that period, if applicable:	Mirion Medical will retain the Customer Personal Data for the duration of this Agreement and for any period after the termination or expiration of this Agreement in accordance with the terms set forth herein or with any applicable legal retention obligations
Sub-Processors	All cases: Cloud-based hosting services are provided by: • Microsoft Corporation, USA[1] • Amazon Web Services. Inc., USA • Amazon Web Services, Germany Mirion Medical Entities not party to the Services Agreement or the Agreement may act as sub-processors to provide additional expertise and resources. Dosimetry services: Outsource Accelerator, Philippines, for the provision of customer support an AR management

[1] (NB: For users of SunCHECK (SaaS): This sub-processor is used only for customers notified of a change of hosting service to this sub-processor and to customers systems installed for the first time after 16 August 2024.)

Schedule 2

Technical and Organizational Measures

Description of the technical and organizational security measures implemented by Mirion Medical:

In **all cases**, the technical and organizational measures described in the Mirion Technologies Cybersecurity and Data Protection Program, available here, apply.

For **dosimetry service**s, the following additional technical and organisational measures are implemented:

BeOSL, TLD and Film Dosimeters

These are dosimeters that are physically sent to Mirion Medical dosimetry services for read-out.

- Raw dose data stored on the dosimeters are encrypted as the dosimeters can only be read out by Mirion Medical dosimetry services using proprietary tools and processes.
- Processing and storage of raw dose data and dose records occur on systems internal to Mirion Medical and secured according to Mirion Medical's Cybersecurity and Data Protection Program available here: https://www.Mirion Medical.com/legal/cybersecurity-and-data-protection-program.
- Data at rest are encrypted.
- Access to data by Mirion Medical personnel is restricted to data required in order to perform assigned tasks.
- Access to dose records by customer personnel occurs through dedicated web services that in turn access the data on the internal servers. Access is strictly restricted to data within the customer account.
- Access to web services by customers is secured by TLS and is restricted to the information and functionality required by the role of the user. Passwords of user accounts have to meet complexity requirements and are stored as a SHA-256 hash in an encrypted database.
- To the extent that servers are hosted by authorized sub-processors, such sub-processors implement adequate technical and organizational measures that are documented in the applicable data processing agreement.

Instadose

These are dosimeters that remain at the customer facility and transmit dose information electronically to Mirion Medical Technologies dosimetry services.

- All data in transit between a data transmission device/software and internal servers are encrypted using TLS 1.2 w/SHA-265.
- Raw dose data are intrinsically encrypted as they can only be transformed into human readable dose records by Mirion Medical proprietary algorithms.
- Raw dose data are not stored on any device/software used to transmit data from the Instadose dosimeter to internal servers. Raw dose data are solely stored in the Instadose dosimeter and on internal servers.
- Devices/software used to transmit raw dose data are hardened by removing all unnecessary components. No remote access to these devices/software is required.
- Instadose data transmission devices authenticate the Instadose dosimeter prior to accepting the raw dose data for transmission.

- Internal servers verify the raw dose data's integrity before accepting it from the transmission device.
- Dose records generated from raw dose data are not accessible from, via or on the Instadose dosimeter.
- Internal servers are accessible only to Mirion Medical personnel and are secured according to Mirion Medical's Cybersecurity and Data Protection Program available here: https://www.Mirion Medical.com/legal/cybersecurity-and-data-protection-program.
- Data at rest are encrypted.
- Access to data by Mirion Medical personnel is restricted to data required in order to perform assigned tasks.
- Access to dose records by customer personnel occurs through dedicated web services that in turn access the data on the internal servers. Access is strictly restricted to data within the customer account.
- Access to web services by customers is secured by TLS and is restricted to the information and functionality required by the role of the user. Passwords of user accounts have to meet complexity requirements and are stored as a SHA-256 hash in an encrypted database.
- To the extent that servers are hosted by authorized sub-processors, such sub-processors implement adequate technical and organizational measures that are documented in the applicable data processing agreement.

For **radiotherapy quality assurance through SunCHECK** the the following additional technical and organisational measures are implemented:

SunCHECK is available through a Software as a Service (SaaS) model and is hosted via Amazon Web Services (AWS). AWS provides critical privacy and security (see https://aws.amazon.com/compliance/hipaa-compliance/) for the presence of Private Healthcare Information (PHI) and Personally Identifiable Information (PII) found within the SunCHECK Platform. The AWS secure environment ensures data is protected and privacy is maintained in compliance with many global data protection requirements.

Security of PHI and PII, for data both at rest and in transit, will be maintained by:

- Access Control:
- Providing a secure connection isolating SunCHECK access to those on the client network and selected Sun Nuclear Support staff only.
- Securing firewall rules from AWS, preventing access to those without permissions to the SunCHECK server.
- Audit Controls:
  Monitors and records user activity (access, changes, deletions, etc.) that contain or use electronic PHI or personal data across the infrastructure.
- Integrity Controls:
- Securing the Virtual Machine for data collection and allowing it access to the AWS database.
- Cisco Advanced Malware Protection (AMP) antivirus on all systems.
- Transmission Security
- Secure site-to-site connection between the customer site and AWS regional data center.
- Safeguards against unauthorized ePHI/personal data access when data is transmitted over the communications network.

Schedule 3

Standard Contractual Clauses

(a) In relation to transfers of Customer Personal Data that is protected by the EU GDPR, the EU SCCs shall apply, completed as follows:

i. Module Two (Controller to Processor) or Module Three (Processor to Processor) will apply (as applicable);

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 2.5 of this Agreement;

iv. in Clause 11, the optional language will not apply;

v. the competent supervisory authority shall be the supervisory authority defined in accordance with Clause 13(a);

vi. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of France;

vii. in Clause 18(b), disputes shall be resolved before the courts of France

viii. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this Agreement; and

ix. Subject to Section 5.2 of this Agreement, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this Agreement;

(b) In relation to transfers of Customer Personal Data protected by the FADP, the EU SCCs will also apply in accordance with paragraph (a) above, with the following modifications:

i. references to "Regulation (EU) 2016/679" shall be interpreted as references to FADP;

ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the FADP;

iii. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law" (as applicable);

iv. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

v. notwithstanding Clause 13(a) the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

vii. in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

viii. Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

(c) In relation to transfers of personal data protected by UK GDPR, the EU SCCs shall: (i) apply as completed in accordance with paragraph (a) above; and (ii) be deemed amended as specified by Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of this Agreement. In addition, tables 1 to 3 in Part 1 of the UK Addendum shall be completed respectively with the information set out in Schedule 1 and 2 of this Agreement and table 4 in Part 1 shall be deemed completed by selecting "neither party".