PRIVACY NOTICE

Effective Date: 05 December 2019

Syneos Health (collectively, "we", "us", "our", or the "Company"), is committed to protecting the privacy of its Associates ("you" or "your") and has implemented the measures identified below to protect the Personal Data we collect and Process. This notice explains how the Company collects and further Processes your Personal Data. This notice does not create an employment contract.

Important Terms

In this notice, the following terms have the following meanings:

- **Associates**: Individuals employed by or contracted by the Data Controller.

- **Data Controller**: The Company entity that is responsible, alone or in combination with another entity, for making decisions about the purpose and means Processing of your Personal Data. The Data Controller is the Syneos Health group entity that employs or engages you. A current list of all Syneos Health entities globally can be found at https://www.syneoshealth.com/our-office-locations. You can contact the Syneos Health entity acting as a data controller through our Global Privacy Office, using the contact information provided in this notice.

- **Personal Data**: The information that relates to you that we Process in connection with your employment with or engagement by the Data Controller. Personal Data includes information that identifies you or permits you to be identified, as well as any other information that can reasonably be linked to you. Personal Data does not include data from which you cannot be identified. Where the definition of Personal Data in this notice conflicts with local privacy law, local privacy law shall control.

- **Process**: Any operation performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as: (i) collection, (ii) recording, (iii) organization, (iv) structuring, (v) storage, (vi) adaptation or alteration, (vii) retrieval, (viii) consultation, (ix) use, (x) disclosure by transmission, (xi) dissemination or otherwise making available, (xii) alignment or combination, (xiii) restriction, (xiv) erasure or destruction.

- **Special Categories of Personal Data**: Certain categories of Personal Data that are subject to special protections under the law and that: (i) reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (ii) include the Processing of genetic data or biometric data for the purpose of uniquely identifying a natural person; (iii) concern your health (including information about disabilities), sex life or sexual orientation; or (iv) are otherwise designated as Special Categories under applicable law.

The Personal Data the Company Collects

We collect Personal Data directly from you, for example, when you fill out a form, provide us with a document, or tell us information about yourself. We may also collect information from third parties, including public databases, social media platforms, professional references, recruitment companies, prior employers, when they provide us with employment references, job board websites you may use to apply for a job with us, or companies performing background checks or ongoing compliance screenings, such as against sanctions or watch lists. Examples of Personal Data we may collect include:

- Demographic data and contact details, such as your name, nationality, race, home address, date of birth, gender, work-related photographs, telephone number, email address, emergency contact details;

- Government-issued identification numbers, such as passport numbers, social security numbers, national identification numbers, driver’s license numbers, or other identification numbers for payroll, administration, and right-to-work purposes;

- Job-related information, such as your curriculum vitae, years of service, hire date, promotion date, employment termination related information, work location, employment ID, work record, vacation and other absences, and contract data;
• Educational and training information, such as your educational and training history, educational awards, degrees, certificates and licenses, transcripts, vocational records and in-house training attendance;

• Recruitment and performance-related data, such as objectives, ratings, comments, feedback results (including from references), career history (including positions held and employers), work equipment, career and succession planning, skills and competencies and other work-related qualifications (such as language skills);

• Credentials and access information, such as your Company email address, usernames, passwords, and keycard number and information related to your usage of the Company’s assets, such as voice mail messages, emails, letters, audit logs and access data, and other deliverables and correspondence created, stored or transmitted by you using computers, networks or communication equipment that is owned or provided by the Company;

• Expenses and travel information, such as information about your business travel and other business expenses;

• Your confirmation and consent to the Company’s various policies;

• Information collected through our security system, such as biometric information and facial images of you when you are in Company facilities collected by our CCTV system and access control system images of you when you are in Company facilities;

• Information needed for business, compliance and risk management, where permitted by law, such as disciplinary records, background check reports, safety and security data, credit and criminal history, drug and alcohol test results, immigration status, right-to-work, visa and residence status, military service status, vehicle registration information, and driving history;

• Payroll and payment or benefits related information, such as salary and insurance information, pension, dependents, government identifier or tax numbers, bank account details, clothing size (for example, to provide certain workers with uniforms or clothing), marital status and beneficiary details, and employment related benefits information (including gender, age, nationality and passport information of your spouse, minor children, and other qualified dependents and beneficiaries);

• Information needed to comply with certain legal requirements, administer benefits, adjustments to work environments, and to assess fitness for work, such as data concerning your health, medical examination reports, information about physical limitations, medical conditions or illness, history of infectious diseases as well as information related to personal and/or physical health (including general health metrics such as height and weight if relevant); and

• Other information you provide to us, such as your feedback and survey responses where you identify yourself.

Where necessary and permitted by applicable law, we may also Process Special Categories of Personal Data, such as data concerning your health (please see “Processing of Special Categories of Personal Data”).

Legal Bases and Processing Purposes

In certain countries, such as the Member States of the European Union, Switzerland and the United Kingdom (upon its withdrawal from the EU), we must inform you about the legal bases and purposes for which the Company Processes Personal Data:

• **To Perform, or Prepare to Perform, a Contract with You.** The Company may Process Personal Data to perform its obligations under agreements with you. For example, we may Process Personal Data for the purposes of: (i) recruitment, hiring and ongoing staffing management; (ii) to Process applications for employment; (iii) to conduct workforce planning (including coordination with third parties); (iv) to administer our workforce; (v) to Process payroll; (vi) to manage compensation and benefits; (vii) to engage in advancement and succession planning and job performance management; and (viii) to provide learning and development opportunities and training.
• **To Comply with Our Legal Obligations.** The Company must comply with the laws of the jurisdictions in which it does business and we may Process Personal Data in the course of complying with such laws. For example, we may be required to comply with requests from law enforcement agencies or in connection with a regulatory investigation or legal proceeding; we may be required to provide Personal Data to tax or other governmental authorities; we may be required to conduct ongoing compliance screening against publicly available watch and sanctions lists; or we may be required to comply with requirements including for compliance with export controls.

• **To Facilitate Our Employment Relationship with You, the Security of our Network, and Other Legitimate Business Interests.** The Company may Process Personal Data for its legitimate business interests, except where doing so would override your interests, rights and freedoms. For example, we may Process Personal Data: (i) to pursue and obtain business; (ii) to engage in workplace management, such as travel and expense programs and internal health and safety programs; (iii) for allocation of work; (iv) to provide for the security of Company facilities and premises, and of Company computers, systems and networks; (v) to establish, exercise or defend legal claims; (vi) to manage compliance with legal and contractual obligations, including participation in audits by sponsors/third parties; (vii) to maintain internal directories; (viii) to conduct employment surveys and engage in general employment management; (ix) to manage internal reporting; (x) to perform internal audits; (xi) to protect the Company, its workforce, and the public against injury, theft, legal liability, fraud, abuse, or threat to the security of our networks, communications, systems, facilities and infrastructure; (xii) to perform our services, corporate governance, and acquisitions; (xiii) to conduct ongoing compliance screening against publicly available watch and sanctions lists; and (xiv) for other customary business-related purposes.

• **With Your Consent.** In specific and well-defined circumstances, we may rely on your consent for Processing Personal Data. Examples include participation in voluntary programs offered by the Company.

From time to time the Company may collect anonymous, aggregated or de-identified data that we use and share to analyze our workforce and business and for other lawful business purposes. Such anonymous, aggregated or de-identified data is not considered Personal Data and is not subject to this notice.

**Processing of Special Categories of Personal Data**

The Company may Process Special Categories of Personal Data with your explicit consent or when the Company is otherwise required or permitted to do so under applicable law. Examples of when the law may permit the Company to Process Special Categories of Personal Data include where the Processing relates to Personal Data you have manifestly made public or where such Processing is necessary to:

- carry out the obligations and exercise the specific rights of the Company or you in the field of employment and social security and social protection law, where permitted by law;
- protect your vital interests or those of another individual where you are physically or legally incapable of giving consent;
- establish, exercise or defend legal claims;
- assess your working capacity, where permitted by law.

**Right to Withdraw Your Consent**

In certain countries, you may have the right under certain circumstances to withdraw your consent to the Company’s Processing of your Personal Data when we Process your Personal Data on the basis of your consent. Once we have received notification that you have withdrawn your consent, we will no longer Process the Personal Data for the purpose(s) to which you originally consented unless there are compelling legitimate grounds that override your interests, rights and freedoms (for example, to comply with a legal obligation), or for the establishment, exercise or defense of legal claims.

If the Company Processed Personal Data for direct marketing purposes, you have the right to object at any time, in which case we will no longer Process your Personal Data for such purposes. The withdrawal of your consent does not affect the lawfulness of such Processing that occurred before its withdrawal.
No Automated Decision Making

The Company does not currently use automated Processing, including profiling, which produces legal effects that concern you or similarly significantly affects you. For example, while the Company may use technology in the operation of the business, the Company does not rely solely on automated algorithms to determine who will be hired, promoted, or terminated.

Monitoring

The Company employs security procedures across its networks, systems, applications and assets and at its facilities. The Company monitors your use of such infrastructure to protect the security of its networks, systems and applications; to protect confidential and proprietary information; to prevent and investigate allegations of injury, theft, fraud, abuse, or other actions giving rise to potential legal liability. Your use of the Company’s computers and systems may be monitored as specified in the Company’s Information Security Policy (Corporate Policy 101). In certain locations, the Company also may employ the use of closed circuit television to monitor its facilities. Any monitoring by the Company of its facilities, networks, systems, applications or assets is performed in accordance with applicable law.

The Way the Company Secures Personal Data

The Company maintains appropriate technical and organizational measures designed to protect your Personal Data against loss or accidental, unlawful or unauthorised, alteration, access, disclosure or use.

Our Retention of Your Personal Data

The Company will retain Personal Data for as long as necessary to fulfil the purposes for which it was collected and Processed, including the period of time required to satisfy any legal, regulatory, accounting or reporting requirements to which we are subject. For example, the Company may be required to preserve Personal Data in connection with litigation, investigations and proceedings, or to comply with a retention period that is established by a local legal requirement.

To determine the appropriate retention period for Personal Data, we will consider the amount, nature, and sensitivity of the Personal Data; the potential risk of harm from unauthorised use or disclosure of the Personal Data; the purposes for which we Processed the Personal Data and whether we can achieve those purposes through other means; and the applicable legal requirements.

Disclosures of Personal Data

The Company may disclose Personal Data to Company departments other than Human Resources, such as Legal, Finance and Information Technology as well as to other Company group entities and third parties for the purposes set forth in this notice.

The parties to whom we disclose your Personal Data include:

- Companies that are members of the Syneos Health Group of companies;
- Joint ventures, subcontractors, vendors or suppliers who perform services on our behalf, such as sponsors, professional advisors (auditors, consultants, lawyers, accountants and other third parties that require your information in the course of providing their services), relocation service providers, background check service providers, payroll processors, travel agencies, benefits providers, insurance companies, business application providers, and other service providers, as well as legal, accounting and other professional services firms;
- Customers and prospective customers, such as sponsors, in the course of pursuing business opportunities and performing our services (for example, your Company bio may be shared on our website or in other publicly available marketing materials and communications as part of our marketing activities);
- A newly formed or acquiring organization if the Company is involved in a merger, sale or a transfer of some or all of its business;
- Any recipient, where the Company is required to do so, such as by court order or by law.
Where the Company discloses Personal Data to third party providers (so called “Processors”), the Company has developed processes and procedures designed to ensure that: (i) it diligently chooses the relevant Processor, (ii) the Processor will only handle Personal Data in accordance with the Company’s instructions, (iii) the Processor is contractually required to adopt adequate technical and organizational measures to protect Personal Data, and (iv) the Processor does not retain Personal Data after completion of its services (save as set out below). Details of the Company’s Processors and the countries in which they are based can be obtained by contacting the Global Privacy Office or its Data Protection Officer.

You are responsible for any additional permissions you choose to grant to Processors for other services. Please note that the Company and its Processors may use Personal Data in an anonymised format (i.e., in a form in which your identity cannot be determined) for other purposes not specified above, including in the development and testing of products and services.

**International Transfers of Personal Data**

Due to the global nature of the Company’s business, the Company may transfer Personal Data to locations where privacy laws may not be deemed by regulators in your location to provide the same level of protections as those in your location. We have taken measures to protect the confidentiality, integrity, availability, and security of Personal Data when it is transferred, and have taken steps to implement an appropriate data transfer mechanism where required.

Certain Syneos Health entities, Syneos Health Clinical, Inc., Syneos Health, LLC, InVentiv Clinical, LLC, InVentiv Health Clinical Research Services, LLC, and InVentiv Health Clinical, LLC (collectively, the “Privacy Shield Entities”), have self-certified to the US Department of Commerce compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Frameworks (“Privacy Shield”) regarding the collection, use, and retention of personal information transferred from the European Union and the United Kingdom and/or Switzerland, as applicable, to the United States in reliance on Privacy Shield. With respect to all Personal Data received or transferred pursuant to Privacy Shield, the Privacy Shield Entities are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. If there is any conflict between the terms in this notice and the Privacy Shield Principles, the Privacy Shield Principles prevail. To learn more about the Privacy Shield program, and to view our certification, please visit [https://www.privacyshield.gov/](https://www.privacyshield.gov/), or contact us through the “How To Contact Us; Raising Concerns” section below and we can provide you with this document. To learn more, please see our [Privacy Shield Statement](#).

Where relevant, the Company uses alternative means of meeting appropriate safeguards for Personal Data transfers outside the EEA, such as executing EU Standard Contractual Clauses or another appropriate data transfer mechanism. You may obtain a copy of the relevant data transfer mechanisms that we have put in place by contacting us through the “How To Contact Us; Raising Concerns” section below.

**Your Rights as a Data Subject**

In certain countries, you may have rights under certain circumstances with regard to our Processing of Personal Data, subject to certain limitations or exclusions provided for under applicable law. These rights may include the right to: (i) access Personal Data and certain information about its Processing; (ii) correct or rectify Personal Data where it is incomplete, inaccurate or outdated; (iii) request the transmission to you of the Personal Data you have provided to us to another Data Controller (iv) object to the Processing of Personal Data, (v) withdraw your consent in relation to our Processing of Personal Data if such Processing was based on your consent (as detailed in the Right to Withdraw Your Consent section of this notice), (vi) delete or erase Personal Data and (vii) restrict Processing of Personal Data.

You may generally exercise these rights free of charge. However, we may charge a reasonable fee or refuse to act on a request, for example, if the request is manifestly unfounded or excessive, in particular because of its repetitive character. It is the Company’s policy to take reasonable steps to verify your identity before acting upon any request you may make to exercise your rights with respect to your Personal Data.

The Privacy Shield Entities further commit to cooperate with the EU data protection authorities (DPAs) for EU employees, the Information Commissioner’s Office for UK employees, and the Swiss Federal Data Protection and Information Commissioner for Swiss employees, with regard to unresolved Privacy Shield
complaints concerning human resources data transferred from the EU or Switzerland, respectively, in the context of the employment relationship.

Your Obligations

It is important that the Personal Data we Process is accurate and current. You should promptly let us know if your Personal Data changes. You may do so by taking advantage of the self-help tools we have made available to you or by contacting your manager, Human Resources, or the Global Privacy Office for assistance.

You must follow the law and the Company’s policies, standards and procedures when handling any Personal Data about others to which you have access in the course of your relationship with the Company. In particular, you must not access or use any such Personal Data for any purpose other than in connection with, and to the extent necessary for, your work with the Company. Your obligation to keep the Personal Data of others confidential continues after the termination of your relationship with the Company.

How To Contact Us; Raising Concerns

We strive to be transparent about how we Process Personal Data. You may contact the Company’s Global Privacy and Data Protection Officer with questions or concerns about the Company’s Processing activities or this notice by email at Data.Privacy@syneoshealth.com, or in writing at Syneos Health, Attn: Global Privacy Office, 1030 Sync Street, Morrisville, NC 27560.

In certain jurisdictions, such as the Member States of the European Union, Switzerland, and the United Kingdom (upon its withdrawal from the EU), you also have the right to make a complaint at any time to your jurisdiction’s privacy regulator (“Supervisory Authority”). Contact information for each EU Supervisory Authority is provided here.

Under certain conditions, more fully described on the Privacy Shield website [https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint], Associates located in the European Union, United Kingdom or Switzerland may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Changes To This Privacy Notice

This notice may be amended from time to time to remain consistent and comply with changes to applicable law or policy, or to clarify our Processing activities. We will notify you once an updated version of this notice becomes available through the Company’s Intranet and/or via an automated message with a link to the notice to your employee email account.