clinicalcomputing

Clinical Computing Inc.

Information Security Framework – Privacy Shield Policy

Date of Release: 11 December 2020

Document Reference: DOC-0141

Review: **Next review Nov 2022**

Table of Contents

1 Introduction

Clinical Computing Inc. is a sister company of Clinical Computing (UK) Ltd:

Name	Relationship	Country
Clinical Computing, Inc.	100% subsidiary	USA
Clinical Computing UK Ltd.	100% Subsidiary	UK

Both companies license clinical information systems, and provide implementation and support services to healthcare organizations. As part of operations both companies will be privy to and receive data on both employees as well as patients when assisting a customer with the implementation and support of its products.

As a supplier of clinical information systems, Clinical Computing assists its clients in the implementation and support of Clinical Computing solutions in their healthcare institution(s). Clinical Computing systems automate the process of managing chronic kidney disease by accumulating data on patient care, maintaining this data in a central repository and providing access to patient data for internal users of clinical information within an institutions IT environment.

As a vendor to healthcare institutions, Clinical Computing supports the requirement to protect patient privacy in all countries in which we do business. In certain countries Clinical Computing also provides managed services such as remote hosting, remote system monitoring, disaster recovery, data warehousing and Application Management Services, in which we act as the intermediary for the protected health information for certain customers. With these offerings Clinical Computing not only has access to provider-based personal health information, but also performs many of a provider's custodial duties. Hosted services are not provided in the EU. It is imperative to provide standards that all Clinical Computing Associates and our Consultants must follow to protect the privacy of patient health information they may come into contact with through the services Clinical Computing provides.

As Clinical Computing (UK) Ltd employs staff in the United Kingdom certain information with respect to our staff may be made available to the US operations in the normal course of business. It is also the purpose of this policy to ensure that employee sensitive data is appropriately managed.

2 Policy Statement

Clinical Computing, Inc. ("CCI") recognizes and acknowledges current data protection laws in the United Kingdom ("UK") and the European Union ("EU"), and has therefore adopted this Privacy Shield Policy ("Policy") governing Personal Data transferred from Clinical Computing (UK) Ltd operations and it's UK and EU subsidiaries, affiliates, agents, third party distributors, patients, customers, dialysis providers and nephrologists or other healthcare providers in the UK and the EU to CCI operations in the United States ("U.S."). This Policy sets forth the standards under which CCI will treat such UK and EU Personal Data.

CCI participates in the U.S.-EU Privacy Shield Framework administered by the U.S. Department of Commerce and commits to abide by the Privacy Shield Principles for all Personal Data received from the UK and the EU. CCI's participation in Privacy Shield is subject to investigation and enforcement by the Federal Trade Commission. For more information about the Privacy Shield Framework, including a list of companies that have certified to Privacy Shield, please visit the U.S. Department of Commerce's website at https://www.privacyshield.gov/.

3 Definitions

"**Data Subject**" means the individual to whom any given EU Personal Data covered by this Policy refers.

"**UK Personal Data**" or "**EU Personal Data**" or "**Personal Data**" means any information relating to an individual residing in the UK or EU that can be used to identify that individual either on its own or in combination with other readily available data (e.g., the individual's name, title, work location, home address, date of birth, compensation, benefits, or family members).

"**Sensitive Personal Data**" means Personal Data regarding any of the following:

- Health or medical condition;
- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Sex life; or
- Criminal convictions or indictments.

4 Contact Information

The following may be used to contact Clinical Computing Inc. or Clinical Computing (UK) Ltd.

Managing Director
Clinical Computing, Inc.
Perseus Operating Group
11350 McCormick Road, Plz 3 Suite 200
Hunt Valley
Maryland 21031
USA

Phone: +1 (513) 3996405

Managing Director,
Clinical Computing (UK) Ltd,
IP City Centre,
1 Bath Street,
Ipswich,
IP2 8SD,
United Kingdom.

Phone: +44 (0)1473 694760

5 Scope and Responsibility

This Policy applies to the collection, use, and disclosure in the U.S. of all UK Personal Data and EU Personal Data transferred from the UK or countries in the EU to CCI in the U.S. Where CCI acts on behalf of group companies as an agent processing UK or EU Personal Data under the direction of CC Ltd., CCI has no direct relationship with the Data Subjects whose Personal Data it processes, and for such Personal Data.

All employees and contractors of CCI that have access to such UK or EU Personal Data in the U.S. are responsible for conducting themselves in accordance with this Policy. Adherence by CCI to this Policy may be limited to the extent required to meet legal,

regulatory, governmental, or national security obligations, but UK and EU Personal Data shall not be collected, used, or disclosed in a manner contrary to this policy without the prior written permission of CCI's Managing Director.

CCI employees and contractors are responsible for engaging third parties to handle UK or EU Personal Data covered by this Policy on behalf of CCI (e.g., temporary staff, independent contractors, sub-contractors, business partners, or vendors) are responsible for obtaining appropriate assurances that such third parties have an obligation to conduct themselves in accordance with the applicable provisions of this Policy, including any applicable contractual assurances required by Privacy Shield. (See 6.4 Accountability for Onward Transfer)

Failure of a CCI employee to comply with this Policy may result in disciplinary action up to and including termination.

6 Privacy Shield Principles

CCI has adopted the U.S. Department of Commerce's Privacy Shield Principles, as set forth below, with respect to the UK Personal Data and EU Personal Data described in the "Scope and Responsibility" section of this Policy that is transferred from operations in the UK or EU to CCI operations in the U.S.

6.1 Privacy Shield Commitment

CCI complies with the EU-U.S. Privacy Shield Framework (Privacy Shield) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and the United Kingdom to the United States in reliance on Privacy Shield. CCI has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect to such information. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

6.2 Notice

CCI takes steps so that Data Subjects covered by this Policy are notified about the types of Personal Data it collects about them, the purposes for which it uses such Personal Data, the types of third parties to which it discloses such Personal Data, the choices and means that it offers for limiting its use and disclosure of such Personal Data, and how Data Subjects can contact CCI with any inquiries or complaints. Notice is provided in clear and conspicuous language at the time of collection or as soon as practicable thereafter; before CCI uses or discloses Personal Data for a purpose other than that for which it was originally collected, and through this Policy.

Specifically, CCI collects and uses Personal Data for, among other things:

1. the delivery of current and future products and services;
2. our everyday business operations such as:
    - product safety and product complaint reporting;
    - customer assistance;
    - business and marketing research;
    - auditing our programs and resources for compliance and security purposes;
3. Employment related purposes and legitimate human resource business reasons such as:
    - carrying out and supporting its human resources functions and activities;
    - carrying out its obligations under employment contracts and employment and benefits laws;

CCI does not disclose Personal Data to third parties with the exception of individuals employed as temporary staff or independent contractors.

CCI will disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

6.3 Choice

In the event EU Personal Data covered by this Policy is to be used for a new purpose that is materially different from the purpose(s) for which the Personal Data was originally collected or subsequently authorized, or is to be transferred to the control of a third party, Data Subjects are given, when feasible and appropriate, an opportunity to choose (opt-out) whether to have their Personal Data so used or transferred. In the event that Sensitive Personal Data is used for a new purpose or transferred to the control of a third party, the Data Subject's explicit consent (opt-in) will be obtained prior to such use or transfer of the Sensitive Personal Data.

6.4 Accountability for Onward Transfer

CCI may share your personal information with third parties including our affiliates and our service providers.

When CCI does disclose personal information, it will do so consistent with any notice provided to Data Subjects and any consent they have given. CCI will transfer Personal Data to such third parties only if the transfer is for limited and specified purposes and the third party will provide at least the same level of privacy protection as is required by this Policy and the Privacy Shield Principles. When CCI has knowledge that a third party is using or sharing Personal Data in a way that is contrary to this Policy, CCI will take reasonable steps to prevent or stop such use or sharing.

With respect to transfers to its agents, CCI remains responsible under the Privacy Shield Principles if an agent processes Personal Data in a manner inconsistent with the Principles, except where CCI is not responsible for the event giving rise to the damage.

6.5 Access

Data Subjects whose Personal Data is covered by this Policy have the right to access such Personal Data and to correct, amend, or delete such Personal Data if they can demonstrate that it is inaccurate or incomplete (except when the burden or expense of providing access, correction, amendment, or deletion would be disproportionate to the risks to the Data Subject's privacy, or where the rights of persons other than the Data Subject would be violated).

6.6 Security

CCI takes reasonable precautions to protect UK Personal Data and EU Personal Data covered by this Policy from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

6.7 Data Integrity and Purpose Limitation

UK Personal Data and EU Personal Data covered by this Policy that is collected, processed, and maintained by CCI shall be kept and used for its intended purpose. CCI takes reasonable steps to ensure that the Personal Data is used for its intended purpose(s), and is accurate, complete, and current.

6.8 Recourse, Enforcement, and Liability

To ensure compliance with these Privacy Shield Principles, CCI will:

- In the investigation and resolution of complaints that cannot be resolved between CCI and the complainant, cooperate with and comply with the dispute resolutions mechanisms of:
    - For HR Personal Data, a panel established by the EU Data Protection Authorities ("DPAs"); and
    - For non-HR Personal Data, a panel established by the EU Data Protection Authorities ("DPAs");
- CCI commits to cooperate with EU data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the UK and the EU in the context of the employment relationship.
- Periodically review and verify its compliance with the Privacy Shield Principles; and
- Remedy issues arising out of any failure to comply with the Privacy Shield Principles.

CCI acknowledges that its failure to provide an annual self-certification to the U.S. Department of Commerce will remove it from the Department's list of Privacy Shield participants, and thereafter transfers of Personal Data will not be allowed unless CCI otherwise complies with EU data protection law.

7 Complaints and Dispute Resolution

In compliance with the Privacy Shield Principles, CCI commits to resolve complaints about our collection or use of your personal information.

UK and EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact the CCI internal complaints mechanism using the contact information provided in section '4 - Contact Information' of this policy.

CCI has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) (an independent recourse mechanism) with regard to unresolved Privacy Shield complaints concerning data transferred from the UK or the EU.

For inquiries or complaints regarding:

- HR Personal Data: the DPA of the UK or EU Member State where the Data Subject works, which can refer the complaint to the DPA panel; or
- Non-HR Personal Data: a panel established by the EU Data Protection Authorities ("DPAs")

Include a statement indicating that your organization commits to cooperate with UK and EU data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the UK or the EU in the context of the employment relationship.

Should a complaint remain fully or partially unresolved after a review by CCI and the applicable independent recourse mechanism, Data Subjects may be able to, under certain conditions, seek binding arbitration before the Privacy Shield Panel. For more information, please visit www.privacyshield.gov.