Data Protection Policy

Policy information	
Organisation	OHI International; OHI
Scope of policy	This policy covers OHI International in Europe overlaps with the GDP in The Orthotic Group in Toronto Canada. – part of the global company OHI Inc
Policy operational date	1/05/2018
Policy prepared by	DPO – Paul Barrett, VP OHI International and Daniel Yu, Director of IT operations in TOG Canada.
Date approved by Board / Management Committee	24/04/2018
Policy review date	Review 01/05/2019

Introduction	
Purpose of policy	Complying with new Government regulations in order to protect clients, staff and other individuals working within OHI International.
Types of data	Medical data pertaining to lower limb kinetics and kinematics.
Policy statement	OHI International have a commitment to all stake holders including patients, that it will comply with both the law and good practice regarding the storage and processing of digital data. We will strive to respect and protect the rights of our customer and their patient at all times and be transparent with all our customers regarding data being stored. All the staff at OHI International receive regular training in data privacy and security and are required to follow the published data privacy and security policies and procedures as published on our manuals.
Key risks	Unauthorized access to protected information by individuals or organisations that are not authorized to view or access this information.

Responsibilities	
The Board / Company Directors	The board of directors for OHI have overall responsibility for data protection within OHI International.
Data Protection Officer	Paul Barrett VP OHI International
Specific Department Heads	N/A
Employees & Volunteers	All members of the OHI workforce are responsible to follow OHI polices and procedures for data privacy and security. They are directed to contact the Data Protection Officer for guidance.
Enforcement	Internal disciplinary procedures.

Security	
Scope	This policy covers all data received, managed, maintained, and transmitted by OHI.
Setting security levels	We are transitioning to a system where all patient level data is de-identified, this change is scheduled to be completed by 25th May 2018. We do not store client financial information. Client demographic information is maintained in the CRM system. Emails are stored on the email server.
Security measures	Servers and workstations are protected by passwords. Passwords must be changed at least once every three months. Workstations are shut down or locked when not in use. All data is stored on the central server and no protected data is stored on the workstations. Hard copies of data are shredded when no longer needed and patient data is de-identified. Access control policies are in place.
Business continuity	Servers that process vital information are attached to backup power supplies. All vital information is backed up weekly and a daily differential is run.
Specific risks	1) email concern https://www.microsoft.com/en-us/TrustCenter/CloudServices/office365/GDPR By default, personal data in transit and at rest is encrypted in Exchange Online, OneDrive for Business, SharePoint Online, and Skype for Business (in Skype-to-Skype voice, video, file transfers and instant messages). To further protect personal data, Office 365 uses multi-engine antimalware scanning to protect incoming, outgoing, and internal messages from malicious software transferred through email. Also by default, Exchange Online uses transport Layer Security (TLS) to encrypt communications between Office 365 and Exchange Online servers and between Exchange Online customers. Microsoft uses platform-level security controls to help ensure the confidentiality, integrity, and availability of customer data, including physical controls, logical controls and data access practices. All access to customer data is monitored, logged, audited, and reviewed by Microsoft. For data breaches on systems governed by Microsoft, Microsoft has a Security Incident Response management and notification process for Office 365. Office 365 is audited at least annually against many global data privacy and network security standards, including ISO/IEC 27001 and 27018. Microsoft regularly tests Office 365 security measures using third-party penetration testing and security audits, as well as industry-standard framework-aligned assessments. Microsoft also operates an Online Services Bug Bounty program, and provides users with development/test environments.

	2) Datacenter (CRM Server Location) https://www.cogecopeer1.com/cogeco-peer-1-renews-its-privacy-shield-certification/ Full back up weekly and daily differential – with offsite replication with Microsoft. 3) GaitScan transfer of data - TCS 2.0 transfers patient/order/scan via HTTPS, with specific TLS 1.2, RSA 2048bits and AES 256 support. For servers, only IT department has full server admin access including the following personnel, Daniel Yu, Yong Yu, Sandor Ge, Charles Chiu, Ian Bonavia, Lei Hua, Jason Tong, Yuri Kondratyev

Data recording and storage	
Accuracy	Servers are frequently monitored and maintained to insure the accuracy and integrity of data stored.
Updating	IT runs a system update every Friday afternoon. Security patches are installed as the patches are released.
Storage	All data is stored on the central OHI server.
Retention periods	Patient data is kept for a period of 7 years.
Archiving	All systems are purged every 6 months of data that is not necessary for the running of the company. All data stored on desktops is saved onto the server at the end of each week and deleted from the workstations.

Right of Access	
Responsibility	OHI is responsible for all data that has been received by OHI. Individuals and organisations that send data to OHI are responsible for sending the data in a secure manner and for de-identifying the patient information.
Procedure for making request	Any requests should be made in writing to the DP assistant.
Provision for verifying identity	This will be verified between the DP officer and the DP assistant and if necessary with the DP officer in TOG in Canada.
Charging	A fee will be based on the administrative cost of providing repeat information.
Procedure for granting access	Proof of account holder validity must be made prior to information being forwarded. This will be checked via a second member of staff. A government issue ID may be requested prior to granting access to information.

Transparency	
Commitment	• All customers have been asked to ensure that patient data sent to OHI Int is de-identified and pseudonymized and that OHI cannot identify the induvial patients for whom the devices are being fabricated. That way the only way to verify the patients details would be through access to the customers electronic system.
Procedure	• Policy documents will be posted on the website and an email will be sent every month for 3 months to remind all customers. • Customers will be notified of policy updates at the time of update and the updated policy will be posted on the OHI website.

Lawful Basis	
Underlying principles	We store orthotic prescriptions for 7 years in case the patient or customer requires a second device or a remake of their original device. That allows us to access the information easily and remake any pairs that might have broken or been deleted by the customer.
Opting out	All our customers have been advised to de-identify the patient name on the prescription forms and all emails and to use a pseudonym or patient ID system. This process ensures that unauthorised access to data will not result in a breech of patient privacy. OHI is not opting out.

Employee training & Acceptance of responsibilities	
Induction	Any new employees will have data protection training as part of their induction.
Continuing training	Training will take place on an annual basis.
Procedure for staff signifying acceptance of policy	Staff will be expected to acknowledge they are happy to undergo, and will comply with, the DPP by ticking an acceptance box on their contract during their annual review.

Policy review	
Responsibility	Paul Barrett and Daniel Yu will be responsible for the policy review.
Procedure	Policy will be reviewed annually with the IT team.
Timing	Review policy every year on the 1st May.