Pilates Health Physiotherapy

Move Well .....Stay Well

PROTECTED HEALTH INFORMATION CLOUD STORAGE RISK ASSESSMENT DOCUMENT

Author: Helen E Hartley, *DPO, Pilates Health Physiotherapy*
Date: 18/02/2019

Terminology:

PHP: Pilates Health Physiotherapy
PHI: Protected Health Information
Associates: All physiotherapy and administrative contractors to PHP
DPO: Data Protection Officer

1. Purpose of Document

1.1 Pilates Health Physiotherapy (PHP) offers one to one clinical appointments and assessments, small group and large group classes for the purposes of educating clients regarding health matters and teaching better postural and movement strategies

1.2 PHP contracts associate physiotherapists and administrative personnel to manage and deliver the above services

1.3 To enable PHP to efficiently run the above services to a professional standard, it is necessary for associates to be able to efficiently and securely share information.

1.4 The purpose of this document is to outline how PHP stores and shares PHI records and steps taken to ensure PHI security

2. Background

2.1 All Physiotherapists working for Pilates Health Physiotherapy are HCPC registered and have CSP membership

HCPC: Health and Care Professions Council
CSP: Chartered Society of Physiotherapists

2.2 Professional bodies such as HCPC and CSP require members to adhere to a code of professional conduct which includes patient confidentiality

2.3 Storage of Protected Health Information (PHI) data forms part of PHP Associate Physiotherapist’s commitment to adhering to this code of professional conduct, whether that PHI is in hard copy, electronic or cloud storage

2.4 In 2016, PHP began using Google Drive cloud storage to store class lists, attendance records, class plans and other administrative documentation. At that time, other than names, there was no other identifiable information stored.

2.5 In 2018, GDPR was introduced in the UK in the form of the Data Protection Act 2018. PHP recognised the need to review our data storage policy and to assess its limitations

2.6 All Associates contracted to PHP are bound by GDPR Data Protection Act 2018

2.7 PHP research (Helen Hartley: DPO) revealed that in the UK there is no specific PHI Legislation on which to base cloud storage compliance. Issues of PHI compliance are covered under GDPR but not specific to either PHI or to cloud storage of such information.

2.8 In the US, there is a PHI compliance standard called the Health Information Portability and Accountability Act (HIPAA 1996) that specifically documents standards for compliance for storing, using and sharing of PHI.

2.9 In 2009, US introduced the Health Information Technology for Economic and Clinical Health (HITECH Act 2009) to specifically address the promotion and expanding the adoption of health information technology.

2.10 GDPR has stringent rules on protection of personal information, but no guidelines on how that relates to using technology or cloud storage

2.11 PHP DPO, Helen Hartley contacted NHS Digital for advice re: cloud storage of PHI. They could give no recommendations - only general advice

2.12 In relation to use of cloud storage, at the date of this report, DPO Helen Hartley could only rely on US HIPAA standards to ensure cloud storage security of PHI with companies such as Google, Dropbox, Amazon S3 Cloud etc

2.13 Following research into differing cloud storage options and what security they offered, Google was as good as any other major cloud storage provider. As Google is based in the US this offers PHI security that met HIPAA standards.

2.14 Google Cloud undergo regular independent verification by several third party auditors and meet EU requirements for personal data storage under GDPR (relevant at time of this report) See 3.6 below

2.15 Data Residency or Geographic data location was also identified as an important part of data storage risk assessment. See 3.7 below

2.16 Consultation with IT specialists and online research indicated that the most ‘at risk’ information security breach lay with the end user. Minimising this security risk appears to be the most important step in meeting GDPR standards for patient information security

3. Research Reference Links

3.1 GDPR & Data Protection Act 2018:
https://ico.org.uk/for-organisations/data-protection-act-2018/
3.2 HIPAA: https://www.hhs.gov/hipaa/for-professionals/index.html
3.3 HITECH:
https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
3.4 HCPC:
https://www.hcpc-uk.org/standards/standards-of-proficiency/physiotherapists/
3.5 NHS Digital: https://digital.nhs.uk/
3.6 Google Compliance
https://support.google.com/googlecloud/answer/6056694?hl=en
3.7 Google Data Residency:
https://www.google.com/about/datacenters/inside/locations/index.html
3.8 G Suite BAA: https://gsuite.google.com/terms/2015/1/hipaa_baa.html
3.9 Various other legal websites with GDPR and PHI information
https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/

4. Steps taken to regulate PHP PHI Storage Safety

4.1 Researched background to Patient Health Information security (see 2 above)

4.2 Purchased G Suite account with Google> research revealed this type of account had a higher level of security as it was HIPAA compliant. Google Drive is not.

4.3 In order to activate HIPAA in G Suite, the administrator (HEH) was required to sign a Business Associate Agreement with Google. This was activated 16th February, 2019

4.4 All previous data stored in Google Drive is now transferred to PHP G Suite account

4.5 Data protection compliance folder created

4.6 Data Protection Officer nominated: Helen Hartley

4.7 Create a data map: identify what information is for administrative use, what information is for clinical use, create folders to reflect this

4.8 Acceptable Use Policy for use of electronic data, including PHI stored in G Suite implemented

4.9 Staff training: GDPR awareness and responsibilities, how to safely and securely use G Suite

4.10 Upload and intermittently review website privacy policy

5. Ongoing Checklist for PHP Safe Storage of PHI Data

5.1 Data protection compliance folder: add to this folder as required

5.2 Data map: monitor the sharing of information. All information movement is tracked in G Suite so is easily identified. Review regularly (minimum each quarter) and log

5.3 Update Health Information biennially as many PHP clients will attend classes over many years and health status may change

5.4 Refresh consent biennially

5.5 Implement Data erasure or correction requests policy

5.6 Review Acceptable Use Policy annually to ensure it meets any changes in standards

5.7 Monitor any changes in G Suite that may affect data security

5.8 Staff training: Ensure new associates are trained to safely use G Suite and educate existing Associates in any changes

5.9 Intermittently review website privacy policy

Table of Contents