Document Name	APC Data Protection Policy
Version	V.3
Approved by	Mani Neelamegan
Approval Date	07 January 2022
Last Reviewed on	01 August 2025

Introduction

Ann Physiocare Limited is committed to safeguard and protect electronic and non-electronic customer data in accordance with GDPR regulations.

In addition, in this policy, the main objective followed by Ann Physiocare Limited, is to establish and maintain adequate and effective security measures for users, to ensure that the confidentiality, integrity and safety all information collected and stored.

Each user has a duty and responsibility to comply with the information protection policies and procedures described in this document.

Essential documents needed to comply with GDPR

Demonstrating compliance with GDPR is one of its manually intensive requirements. We complete dozens of documents to prove that you have the necessary policies and procedures in place, and although you might understand the GDPR, it doesn't necessarily mean that you can produce this documentation.

Data Protection Impact Assessments (DPIAs)

GDPR states that Data Protection Impact Assessments are necessary for projects that are "likely to result in a high risk to the rights and freedoms of natural persons". By completing DPIAs, you can identify and examine the project's potential effects on individual privacy and compliance with data protection legislation. The Article 29 Working Party believes that DPIAs should always be carried out before processing and become part of a proactive "privacy by design" approach.

Consent Forms

A common misconception of the GDPR is that you need to get consent to process personal data. In fact, there are six lawful grounds for processing data and consent is the riskiest and least favorable. Still, there will be times when it's the only option, so you need to produce GDPR-compliant consent forms. This means you need to:

1) Request as little data as possible: Data should be collected for a specific purpose, used only for that purpose and retained for only as long as it meets that purpose. You'll typically need individuals' names and contact information at the very least, but you must decide what other information, if any, is necessary for the task at hand.

2) Make the terms and conditions clear: You can't hide the terms and conditions for consent, and you can't make them so vague or complicated that people won't read or understand them. Consent mechanisms must be easy to use and kept separate from other terms and conditions, and requests must be written clearly and concisely.

3) Make it easy to withdraw consent: Consent requests need to make it as easy (or easier) for individuals to withdraw their consent as it is for them to give it. This means individuals need to be told straight away that they can withdraw their consent at any time, and you must explain how to do it.

A Description of the Data Protection Officer Role

Although only some organisations need to appoint a Data Protection Officer (DPO), the WP29 advises all organisations to appoint one as a matter of good practice. The DPO has a variety of tasks, and organisations should use this document to establish their remit. This will help the DPO, management and staff understand how the organisation is meeting the GDPR's requirements.

Data Protection Policy

It's essential that staff know how to process data lawfully and who to approach if they have any questions. A data protection policy should cover both of these elements. Having a DPO will be beneficial for both of these, as they are responsible for making sure that staff comply with the policy.

Data Breach Notification Procedure

The GDPR defines a data breach as the accidental or unauthorised destruction, loss, alteration, disclosure of or access to personal data. Organisations need to report a breach when it is likely to risk the rights and freedoms of individuals. This covers significant economic or social disadvantages, such as discrimination, reputational damage or financial losses.

Any breach that meets these requirements must be reported within 72 hours of discovery. To achieve this, all employees, contractors, temporary staff and third parties need to be aware of, and follow, a data breach notification procedure.

Subject Access Request (SAR) forms and Procedures

Under the GDPR, all organisations need to give individuals the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information (mostly the information provided in privacy notices).

The procedure for making and responding to subject access requests remains similar to most current data protection laws, but the GDPR introduces some changes.

Administrative Security Measures

1. Designation of an information security coordinator / committee

2. Ongoing employee training on security and information management

3. Disciplinary measures for violations of the program

4. Procedure for ensuring that terminated employees no longer have access to personal information

5. Procedures for the storage, access and transfer of personal information outside of the company

6. Procedures for selecting appropriate third-party service providers and obtaining written agreements from them to ensure that personal information receives adequate protection

7. Procedures for limiting access to personal information to the individuals that require access to accomplish a legitimate business purpose

8. Routine review of company compliance with the program

9. Monitoring the program regularly to ensure that it is adequately preventing unauthorized access

10. Reviewing the program, at least annually, to determine whether it requires revision in light of new threats or technologies

11. Procedure for documenting the company's response to security breaches

Physical Security Measures

Reasonable restrictions on physical access to personal information, such as keeping personal information in locked facilities, storage areas or containers.

Electronic Security Measures.

1. Routine monitoring of computer systems for unauthorized access.

2. Reasonably up-to-date network firewall protection.

3. Reasonably up-to-date virus and malware protection.

4. Reasonably up-to-date system software.

5. set up to receive regular software security updates.

6. Policies that require the use of unique user names to access personal information.

7. Reasonable procedures for selecting passwords of appropriate complexity and strength.

8. Use of encryption to protect personal information, including the encryption of emails, file transfers, laptop computers or mobile devices that contain personal information.

Adding to the difficulty of this task is the fact that new risks, exploits and security breaches are discovered every day as are new, effective solutions to those problems. It is important for information security coordinators to keep up-to-date on recent news, security incidents and industry standards.

The core challenge for a company developing an information security program is identifying the reasonably foreseeable threats and adopting appropriate security measures to mitigate those risks. It may

not be possible to protect against all potential threats, but companies will need to identify threats that are reasonably foreseeable.

How do I dispose of personal information in a way that complies with the law?

All affected individuals, businesses and agencies must meet minimum standards for disposal of personal information.

- Paper documents must be redacted, burned, pulverized or shredded so that the personal information cannot practicably be read or reconstructed.

- Electronic files, disks, hard drives or other storage media must be securely destroyed or erased so that the personal information practicably cannot be recovered after disposal.

What is a data security breach?

A data security breach is considered to be any loss of, or unauthorised access to, Ann Physiocare Ltd's data normally involving Personal Medical or Confidential information1 including intellectual property. Data security breaches include the loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, human error (e.g information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.

Personal information is defined as any information relating to a living individual who can be identified either from the data or from that information used in conjunction with other information that may be available.

Confidential information is privileged or proprietary information that could cause harm (including reputational damage) to the University or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure.

Managing a data security breach

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. Breaches can result in

fines of up to £20,000,000 for loss of personal information and significant reputational damage, and may require substantial time and resources to rectify the breach. The following procedure outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently.

This procedure outlines the four stages (4.2 to 4.6 below) which should be completed following the initial containment of the breach. The individual stages may run concurrently.

Record keeping

Throughout the breach management process records should be kept of what action has been taken and by whom. Appendix C provides an activity log template to record this information, in addition copies of any correspondence relating to the breach should be retained.

Security breach procedure

Containment & recovery

As soon as a data security breach has been detected or is suspected the following steps should be taken:

- Identify who should lead on investigating and managing the breach
- Establish who (within Ann Physiocare Ltd.) should be aware of the breach – you must contact the Compliance Team or Lead Therapist

Identify and implement any steps required to contain the breach.

- Identify and implement any steps required to recover any losses and limit the damage of the breach
- If appropriate inform the police/insurance office

Assessment of risk

All data security breaches must be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach should be assessed in order to identify an appropriate

response. The checklist in Appendix A should be used to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

Notification of breach

Consideration is required as to whether any individuals, third parties or other stakeholders should be notified of the breach. This will depend on the nature of the breach, any notification must be carefully managed. Don't be too quick to disclose information before the full extent of the breach is understood; when disclosure is required ensure that it is clear, complete and serves a purpose. The checklist in Appendix B: Notification of breach checklist should be used to identify potential stakeholders who should be notified and to establish what information should be disclosed.

The Lead Therapist or other senior manager must be involved in the notification process and no message sent without approval. The Information Commissioner's Office may be notified only after liaison with the Ann Physiocare Ltd.'s Data Protection Officer.

Evaluation and response

It is important to investigate the causes of the breach and evaluate Ann Physiocare Ltd.'s response to the breach. A brief report on the breach, how it was dealt with and recommendations on how to prevent the breach reoccurring and similar risks should be written.

Finally if there are recommended changes to this procedure, such as additional information that would have been helpful or further explanation required these should be communicated to Ann Physiocare Ltd.'s Compliance Officer.

Further resources and contact details

Resources

- ICO guidance on Data Security Breach Management

- Notification of Data Security Breaches to the ICO

APPENDIX A:

SECURITY BREACH RISK ASSESSMENT CHECKLIST

a) What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)

b) How did the breach occur?

c) What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)

d) How many individuals or records are involved?

e) If the breach involved personal data, who are the individuals? (Patients, staff, therapists etc)?

f) What has happened to the data?

g) Establish a timeline? (When did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)

h) Were there any protections in place? (e.g. Encryption)

i) What are the potential adverse consequences for individuals or Ann Physiocare Ltd.? How serious or substantial are they and how likely are they to occur?

j) What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?

k) What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted)

~ Policy Implementation Notice ~

This is the policy statement of:

ANN PHYSIOCARE LIMITED

The overall and final responsibility for this policy is that of:

DIRECTOR

Signed: 

Dated **01/08/2024**

Day-to-day responsibility for ensuring this policy is put into practice is delegated to:

MANI NEELAMEGAN

Policy Review Date: 01/08/2025

Next Review Date: 01/08/2026