Policy Relating to Accidental Disclosure of Confidential Information

The Pepper Clinics

At The Pepper Clinics we are aware of Article 5 (1) (f) of the General Data Protection Regulation which states that personal data shall be:

> "…protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

If a Data Breach occurs, we would take the following steps:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

Containment and Recovery

As soon as a breach of confidentiality is discovered, we would assign a person to be responsible for ensuring that the breach is documented using our Data Breach template, and contained. We would establish who needs to be aware of the breach and how they can help in containing it. This may involve shutting down computer systems or establishing new access codes, finding new safe storage for record cards, or changing locks on doors.

We would act to recover any lost or corrupted data as soon as possible using backup tapes/restoring lost or damaged data.

Assessment of Ongoing Risk

We would access the type of data involved and its level of sensitivity. We would also assess how much data was involved and the number of people affected.

We would endeavour to find out what has happened to the data and if stolen, whether it could be used harmfully. We would assess whether the data could lead to physical risk, significant distress or damage for the people involved. We would also assess whether the information could lead to identity fraud or financial loss.

Dependent on the type of data we would also assess the damage to the reputation of the practice.

Notification of Breach

We would decide who needed to be informed of the breach. This would be based on who was involved and the type of information. We would make sure that we were meeting our security obligations with regard to the principles set out in Article 5 of the GDPR. We would also make sure we have a clear purpose as to our reasons for notifying affected individuals.

If we felt it was appropriate in that:

- The volume or nature of data loss was significant;
- The data related to children or vulnerable persons;
- The data was likely to cause significant distress or damage to individuals;

- The data was likely to incur significant reputational damage to the practice

- Then we would consider making notification as appropriate to:
- The Information Commissioner (within 72 hours of discovery)
- Healthcare regulator
- NHS authorities

We would discuss with our defence organisation how we should inform the people affected by the breach and what we should say to them. We would make sure we had a contact point in the practice for anybody who had queries to be able to contact.

If it was felt necessary we would inform the ICO. For guidance on whether to inform them we would go to www.ico.org.uk

Evaluation and Response

We would investigate the cause of the breach and how we responded to it. We would review all aspects and update our policies and procedures in light of what we found.

We would ensure that our Data Breach template was completed for every breach, no matter how apparently slight or insignificant, so that we could learn from every issue and take appropriate corrective action for the future.

We would look for any weak points in our system and work to improve them. This may involve further training of staff, assignation of responsibilities and ongoing monitoring.

March 2019

Review March 2020