Distinctive Dentistry Ltd
Policy Relating to Accidental Disclosure of Confidential Information

Reviewed January 2019

At Distinctive Dentistry 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 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 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 pass codes, finding new, safe storage for record cards or changing door locks.

We would act to recover any lost or corrupted data as soon as possible using off site back up if the loss/breach was related to our computer records.

Assessment of ongoing risk

We would assess the type of data involved and it's sensitivity. We would also assess how much data was involved and the number of people affected.

We would endeavour to find out what had happened to the data and if stolen, whether it could be used harmfully. We would assess whether the data could lead to physical risk or damage of reputation 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 data involved. We would make sure that we were meeting our security obligations with regard to article 5 of the GDPR. We would also make sure that we had a clear purpose as to our reasons for notifying 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

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

If it was felt necessary we would inform the ICO. For guidance on this we would go to

www.ico.gov.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 the light of what we found.

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

To review Jan 2020 or if relevant change