1. References:

- Guidance on data security breach management ICO 2017
- Record and record Keeping Policy
- Consent to release information policy
- Data Protection Policy
- Information Sharing Policy
- Information Technology Policy
- Security Policy
- Data Protection Act 1998, Privacy and Confidentiality Law and Information Sharing Best Practice
- GDPR 2018
- Freedom of Information Act 2000
- Records Management Best Practice and Standards and Copyright Law
- Information Security and Information Risk Standards
- Information Quality Assurance Best Practice

2. Scope:

- All information held within EnViva Complex Care offices.
- All information systems operated or managed by EnViva Complex Care.
- Any individuals using information held by EnViva Complex Care.
- Any individual requiring access to information held by EnViva Complex Care.

3. Policy Statement:

The purpose of this document is to outline an information governance framework that ensures EnViva Complex Care: -

- Meets its legal obligations for effective management of information
- Recognises the key enabling role of information in supporting the achievements of company objectives
- Ensures that information is treated as a valuable asset
- Clarifies our belief in transparency
- Identifies our process in proactively managing Information Governance breaches and implementing lessons learned from these.

4. Overview:

Information is a vital asset, both for the provision of services and for the efficient management of services and resources. Without it, informed substantiated decisions cannot be made. It is paramount that information is efficiently managed, and that appropriate standards, policies and procedures provide a robust governance framework for information management.

The Objectives:

EnViva Complex Care objectives are to ensure that they:

- Hold information securely and confidentially
- Obtain information fairly and efficiently
- Record information accurately and ethically
- Share information appropriately and lawfully
- will aim to ensure that information is available to support a quality service for all clients and staff, by adopting a culture of openness, transparency and accountability.

Responsibilities

The Quality Assurance Manager and the Director of Care are responsible for Information Governance. This includes agreeing related policies and agreeing implementation methods and improvement plans. The improvement plans will include the following:

- **Training and Awareness**
  Each department will have a planned approach to Information Governance awareness including training for all related policies and procedures. This should be work related training and regularly assessed to ensure that all employees are equipped with the relevant skills to fulfil their responsibilities. Training will be given at induction and annually updated for all employees. Additional communication is shared through employee Newsletters and staff meetings.

- **Document Procedures**
  There will be documented procedures to support the agreed policies; these will specify any operational instructions required to ensure compliance with legislation and standards

- **Monitoring and Compliance**
  There will be regular effective monitoring of compliance through audit by the Quality Assurance Manager and Heads of Department.

- **Data security breach management Strategy**
  Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Many organisations take the view that one of those measures might be the adoption of a policy on dealing with a data security breach.

  A data security breach can happen for a number of reasons:
  - Loss or theft of data or equipment on which data is stored
  - Inappropriate access controls allowing unauthorised use
  - Equipment failure
  - Human error
  - Unforeseen circumstances such as a fire or flood
  - Hacking attack
  - 'Blagging' offences where information is obtained by deceiving the organisation who holds it

There are four important elements to any breach management plan:
Containment and recovery, Assessment of ongoing risk, Notification of breach, Evaluation and response

1. <u>Containment and recovery:</u>

All near misses/data breaches must be reported in accordance with our Incident reporting policy. All Information Governance related incidents are recorded as a "Security Incident". Following our incident reporting procedure, the severity of the breach will be ascertained by an assigned member of the senior management team who will act as lead investigator during our subsequent investigation.

- Sensitive detail lost through human error such as email/telephone/post: Contact must be made with the person receiving the data immediately, requesting that they return the data (or delete the data if sent electronically) and confirm this has occurred.
- Lost/stolen equipment or unauthorised access, immediate reporting to the IT department will be required, in order to implement account closure, access termination and electronic. If appropriate the Police may need to be notified.

2. Assessment of ongoing risk:

Not all breaches will require extensive action; attention must focus on the severity of the incident and adverse consequences for the individuals involved. The lead investigator will need to determine the following:

- What type of data is involved? How sensitive is it? Some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption? What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
- Who are the individuals whose data has been breached? Whether they are staff, customers, service users or suppliers, for example, will to some extent determine the level of risk posed by the breach and actions in attempting to mitigate those risks.
- What harm can come to these individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in our service and provision?
- If individuals' bank details have been lost, additional support may be provided by contacting the bank etc. for advice on preventing fraudulent use.

2. Notification of breach:

Convivium Care remains clear in its obligations to its clients, customers and staff, transparency is key to ensuring we meet our legal and ethical obligations.

Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal effectively with complaints.

When considering notification to external sources, the following must be determined:

- Are there any legal or contractual requirements? Specific services or contracts may require reporting of such breaches or near-miss events.
- Whether the matter needs to be reported to the Information Commissioners Office (ICO) under the GDPR
- What additional support may be needed to support individuals affected such as vulnerable adults or children.

Where appropriate verbal (initial contact) and written contact should be made to all parties involved in the breach providing them with assurance of our actions, details of our investigation and errors made. Transparency remains central in this process to ensure damaged trust can be rebuilt.

3. Evaluation and response:

EnViva Complex Care remains committed to learning from our errors, ensuring we continually improve the services we deliver. Whilst we acknowledge a culture of 'no blame' we expect our employees to be diligent in their day to day activities and fully understand their responsibilities to ensuring data is kept safe. We are focused on promoting a culture where all employees ensure they get it "right first time" to ensure our data is stored, accessed and shared appropriately.

All Information Governance related incidents are recorded as "security incidents" and reported to the Quality Assurance Manager/Director of Care immediately and subsequently by the Operations Director at the Board of Directors meeting. In addition, all regional and departmental meetings will use such breaches/near misses as case studies to cascade learning. This enables all incidents to be shared across all departments.

External reporting

EnViva Complex Care is registered with the Information Commissioners Office (ICO reference Z765103X).

In accordance with their regulatory advice any breaches involving large numbers of individuals will be reported directly to them.

Procedure Review		
Review Date	Sections changed	Reasons