Readily Accessible and Secure retention of records Policies and Procedures.

Training:

Keystone Healthcare understand the importance of securely retaining records whilst ensuring they are easily available.

All office workers involved in this process will receive appropriate formal training prior to engaging in this process on these policies and procedures and GDPR to ensure compliance with these procedures is fully understood and met.

This document will also be available to all workers for reference in the document management system.

Auditing:

As part of our commitment to continual improvement these policies and procedures will be audited for effectiveness and compliance on at least an annual basis. This will then be part of our annual management review.

Verification of readily accessible records

As part of our business activity we must keep personnel and financial records in order to run the business effectively and to comply with statutory and client requirements.

Keystone Healthcare operate a transparent policy in order to satisfy the requirements of the authority/participating authority. This includes ensuring that all information, data and other records and documents required are made readily available to the Authority in the format and in accordance with any timescales set out in the Services description.

Keystone Healthcare are current registered with the I.C.O, ensuring that all policies and processes are set in line with guidance supplied. **I.C.O. Registration No: Z1062653** (Certificate attached.)

In order to achieve this, Keystone Healthcare obtain consent from each candidate at registration stage that their personal data can be made readily available and accessible by the relevant and necessary parties, including auditors; participating authorities and any other relevant third parties.

The type of record will determine the length of time we must retain the records for. All records we hold are kept in line with Data Protection Laws.

Keystone Healthcare have developed a Record Management Program in accordance with the following acts:

- The Access to Health Records Act (1990)
- The Data Protection Act (1998)
- Freedom of Information Scotland Act (2002)
- Public Records Act (Scotland) 2011
- Regulation 29 of the Conduct Regulations and Data Protection

Authority of this policy
This policy has been authorised by Richard Ward – Managing Director and registered Data Controller and is available to all staff. It has been developed in consultation with staff and will be revised on a regular basis. Ownership of the policy rests with Richard Ward.

Scope
All staff, Board members volunteers, contractors and consultants etc must comply with this policy, in their conduct of official business for Keystone Healthcare. This policy applies to records in all formats, including electronic records.

Records as a resource
Keystone Healthcare recognises that records are a vital asset to:

- facilitate information accessibility, and enhance business by supporting program delivery, management and administration
- deliver customer services in an efficient, fair and equitable manner
- provide evidence of actions and decisions and precedents for future decision making, and
- a small percentage of Keystone Healthcare records will become archived

Records Management Program

Objectives of the Records Management Program
A records management program is a planned, coordinated set of policies, procedures, people, systems and activities that are required to manage records.

The Keystone Healthcare Records Management Program seeks to ensure that

- it has the records it needs to support and enhance ongoing business and customer service, meet accountability requirements
- these records are managed efficiently and can be easily accessed and used for as long as they are required
- records are stored as cost-effectively as possible and when no longer required they are disposed of in a timely and efficient manner

A goal of particular note is that the organisation is committed, through its Records Management Program, to maintaining digital and other technology dependent records in authentic and accessible form for as long as they are required.

Storage

Current hardcopy records should be stored in [designated storage areas for current records] in locked cabinets with access restrictions.

Rarely used records or records no longer in use for official purposes that are still required to be retained should be forwarded to Richard Ward – Managing Director / Data Controller.

Electronic records are stored in our encrypted and password protected compliance system.

Appropriate access levels are set for office staff ensuring they only have access to records appropriate to their roll.

Records of short-term value will be disposed of at suitable intervals by Richard Ward – Managing Director / Data Controller. Records of long term or archival value will be retained online with timescales in this policy.

Access

Data protection and consent to retain store and audit records including 3rd party auditor's information is obtained from each candidate during the recruitment phase.

Records are made available to all authorised staff that require access to them for business purposes. Relevant access rights are granted by the data controller.

All access to Keystone Healthcare records by members of the public, including Freedom of Information requests, will be in accordance with:

- The Access to Health Records Act (1990)
- The Data Protection Act (1998)
- Freedom of Information Scotland Act (2002)
- Public Records Act (Scotland) 2011
- Regulation 29 of the Conduct Regulations and Data Protection

Regulation 29

Keystone Healthcare abides by the clauses/terms as set out within regulation 29 of the conduct Regulations and Data Protection (Guidance taken from legislation.gov.uk)

All records are retained securely but are easily accessible.

We will retain and delete your personal data as follows:

(a) Account Data will be retained for 6 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

(b) Profile Data (other than Profile Data which is also Account Data) will be retained for 6 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

(c) Contact Data (other than Contact Data which is also Account Data) will be retained for 2 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

(d) Usage Data will be retained for 2 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

(e) Enquiry Data (other than Enquiry Data which is also Account Data) will be retained for 2 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

(f) Transaction Data will be retained for 2 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

(g) Notification Data (other than Notification Data which is also Account Data) will be retained for 2 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

(h) Correspondence Data (other than Correspondence Data which is also Account Data) will be retained for 2 years following the date of our last contact or dealing with you, at the end of which period it will be deleted from our systems.

Exceptions – Any information relating to NHS contracts

- This information will be held for minimum of 6 years after the conclusion of any contract, or such longer period as agreed between the parties. Full and accurate records of all matters relating to each contract are retained in order to deal with any civil action in form of contractual claim (Limitation Act 1980)

- Where any records could be relevant to a claim for personal injury such records shall be kept secure and maintained for a period of twenty one (21) years from the date of end of any Contract.

Amendments

- We may update this policy from time to time by publishing a new version on our website.

- You should check this page occasionally to ensure you are happy with any changes to this policy.
- We may notify you of changes to this policy by email.

Keystone Healthcare's Privacy Notice is available on request and can be found on the website:
https://www.keystonehealthcaregroup.co.uk/app/uploads/2019/10/Privacy-Notice.pdf

Further information

Further information regarding GDPR can be found in the NHS Employers GDPR section which can be accessed in full here:

https://www.nhsemployers.org/your-workforce/recruit/employment-checks/gdpr-guidance

Retaining and Recording Information

Information relating to appointments are recorded in Keystones Compliance database and in hard copy files in line with the Data Protection Act 2018 (Underpinned by the General Data Protection Regulations 2018)

Any information gathered is retained for the minimum periods outlined within the codes of practice for handling information in health and social care which can be found on NHS Digital's website.

You can contact us:

(a) by post, using the postal address given above;

(b) using our website contact form;

(c) by telephone, on the contact number published on our website from time to time; or

(d) by email, using the email address published on our website from time to time.

Data protection officer

Our data protection officer is Richard Ward, who can be contacted via email: richard@keystonehealthcaregroup.co.uk, or telephone: 01484545990.

Review

This policy will be reviewed annually or if legislation changes within this timeframe