PAS Introduction - Data Protection and Security Guidelines

PAS Introduction - Data Protection and Security Guidelines

The Data Protection Act 2018 (UK variant of the wider European General data Protection Regulation)

The DPA18 applies to a wide definition of personal data, in short "any information relating to" an individual (i.e. includes identifiers such as name, ID numbers, phone number, online ID, mobile device ID, or one or more factors about an individual's physical, physiological, genetic, mental, economic, cultural or social identity). Pseudonymised data will also be classed as identifiable and should be afforded the same levels of confidentiality.

Six privacy principles for handling Personal Identifiable Data

1. **Lawfulness, fairness and transparency:**
   Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)]. If you are unsure about the lawfulness of your processing please contact rch-tr.infogov@nhs.net for support and advice.
2. **Purpose limitations:**
   Personal data can only be obtained for "specified, explicit and legitimate purposes"[article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.
3. **Data minimisation:**
   Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the

minimum amount of data should be kept for specific processing.

4. **Accuracy:**
   Data must be “accurate and where necessary kept up to date” [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.
5. **Storage limitations:**
   Regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary” [article 5, clause 1(e)]. In summary, data no longer required should be removed.
6. **Integrity and confidentiality:**
   Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage” [article 5, clause 1(f)].

Your obligations

- Passwords are used to restrict access – Do not divulge your password to anyone.
- Do not allow others to use your account.
- Lock portable computers in a desk or filing cabinet.
- Do not leave any member of staff, including members of the IT department, unattended in an area where personal data is stored/recorded.
- Treat all printouts as if it were a page from the patient health record.
- Mark email as [secure] when sending emails with confidential information to non-nhs.net accounts.
- Electronic media (e.g. CD’s/ DVD’s) must be encrypted before leaving the department.
- Always dispose of unwanted printouts safely, using a shredding machine or equivalent.

Patient Confidentiality

- It may be necessary during the course of their work for staff to read part of the contents of the health record or access data which is electronically stored but this should only be as much as is absolutely necessary in the efficient performance of their duties.
- Staff must never leave a PC or terminal logged on while unattended – you are responsible for all actions carried out under your password.
- Under no circumstances should staff access their own data or that of friends, family, colleagues.
- Staff will not Request or handle their own case notes but may make an application to see their records under the Access to Health Records Procedure.
- Staff must never use confidential information for any purpose that does not conform to those purposes authorised by the Trust.
- Staff must never use personal or corporate data or equipment for personal gain.
- Please note that any breach of confidentiality will be regarded as a disciplinary offence and may result in dismissal.

REMEMBER

- Treat all personal (both staff and patient) information with care
- Ignorance of the Act is no excuse
- Do not pass on personal information to unauthorised persons
- If you cause a breach or become aware of a breach of confidentiality, please login on Datix and report it to Information Governance using the email address below.
- If in doubt ASK! Please contact Information Governance for advice using the email address below.

Information Governance Contact

The Information Governance email address: rch-tr.infogov@nhs.net.