Standards – Guidance and Examples

Data

Standard

4.1 Data Integrity & Security

Rationale

PASA requires the provider to demonstrate their policy for ensuring data is kept securely and that they meet requirements of the Data Protection Act 1998. In addition to ensuring the security of data, administrators need to prove they can demonstrate the integrity of data and how they can maintain it in order meet the Pensions Regulator's data quality standards.

Outcomes

- Administrators are able to pay the correct benefits at the right time to the right person;
- members of pension schemes' data is held securely and is not open to risk of disclosure inadvertently or maliciously.

Measurement / Evidence

- Providers should have in place the ISO 27001 Data security standard;
- employees should be required to read and agree to adhere to the company's data security policy;
- a data security protocol is in place and regularly refreshed;
- staff undertake data protection refresher training on a biennial basis;
- process and procedures should be in place to monitor and review the data security policy to ensure the policy remain relevant for the organisation in terms of services offered and business strategy;
- a dedicated data security officer should be in place to ensure compliance with the policy;

- the provider should regularly run data analysis tools to ensure that the data integrity is maintained, for example during a scheme migration, a bulk upload of data and part of the annual renewal;
- data import protocols should include data validation, for example interfaces files, web access;
- system user access protocols should be in place;
- data quality reporting should be part of the annual or quarterly stewardship reporting.

Measurement / Evidence

PASA believes that a documented Data Security Policy is a requirement for an administration organisation.

Providers need to be able to demonstrate that their data security policy is clearly defined and maintained; that they are monitoring the plan to ensure it remains fit for purpose; and that they are proactive in ensuring that staff are aware of their responsibility for the security of client data.

PASA believes that once data has been analysed and cleansed, the providers should ensure that it remains of a high quality and that the integrity is not affected by undertaking day today administration.

Application to TPAs and Accreditation Approach

The accreditation team will review:

- evidence of a documented data security policy;
- evidence of that employees are aware of the policy and the implications of not complying;
- evidence of the data analyse tools and capabilities;
- evidence of system access levels;
- evidence of separation of client data;
- evidence of the validation capabilities of data import/export capabilities.

Application to In House Teams and Accreditation Approach

The accreditation team will look for:

- evidence of a documented data security policy;
- evidence of that employees are aware of the policy and the implications of not complying;

- evidence of the data analyse tools and capabilities;
- evidence of system access levels;
- evidence of separation of client data;
- evidence of the validation capabilities of data import/export capabilities.

Timeline

PASA expects this standards to be applied immediately