Standards – Guidance and Examples

Data

Standard

4.1 Member Data Quality Standard

PASA expects administrators to have robust data[1] quality and data management procedures in place to ensure the accuracy, completeness and security of member data both with operating systems, on transfer of data and around data access both within the operation and via remote and website based access.

Rationale

The administrator is able to demonstrate their policy for ensuring the highest level of member data quality standards are achieved and maintained for their Principals, supporting the effective delivery of administration services and compliance to regulatory and legislative requirements.

General Principles

PASA believes that a documented Data Management Strategy/Policy is necessary for and supportive of a robust administration service.

Providers need to be able to demonstrate that their data management strategy/policy is clearly defined, implemented 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 quality of their Principals' data.

PASA believes that once data has been analysed and cleansed, that providers should work with their clients to ensure that data remains of a high quality. PASA also believes that providers must ensure that the integrity of recorded data is not affected by undertaking day to day administration.

Where some or all services are outsourced to a third party provider, PASA expects the appointee to have an appropriate and suitable data management strategy and policy in place and to report on it to the delegating party.

[1] Data is expressed to include member data, scheme data, client data, policyholder data, confidential information and any data of a sensitive nature

Outcomes

Outcomes should support the following:

- Accurate payments of benefits to members;
- Timely settlement of member and survivor benefits;
- Effective communication to members;
- Member data is held and transmitted securely and is protected from corruption and unauthorised disclosure;
- Effective management and mitigation of risk, including fraud risk;
- Compliance to tPR common and conditional data regulation, Client Confidentiality requirements of any governing bodies and General Data Protection Act (GDPR) requirements.

Measures/Evidence

The administrator must have a documented Data Management Policy which evidences the data security and integrity policy of the provider. The administrator should be able to evidence that staff have been made aware of their obligations to protect data and have been appraised of their ongoing obligations under the GDPR regulations to ensure that data is protected, handled confidentially and that any data transmitted is suitably protected from corruption and any fraudulent activity, in accordance with the provider's policy.

Where some or all services are outsourced to a third party provider, PASA expects the appointee to have an appropriate and suitable data management strategy and policy documented and in place and that these requirements are reflected in the agreement between the parties.

Application to TPAs and Accreditation Approach

The accreditation team will review:

- Evidence of a documented data management policy, to include data security protocols for the transfer of data, including evidence of data mapping, risk identification and adoption of procedures to minimise potential risk;
- That a Data Protection Officer has been appointed; if required;
- How the TPA facilitated the measurement, metrics and procedures to achieve the data standards;
- Evidence of ongoing training so that employees are aware of data protection requirements and the implications of not complying;

- Evidence of the data analysis tools used and the results of any reviews undertaken;
- Evidence of systems access limitations, how these are managed and how access rights have been closed down for leavers of where access for an individual is no longer relevant to their role;
- Evidence of the segregation of client data;
- Evidence of appropriate mortality screening and 'living as stated' activity and results;
- Evidence of fraud risk identification and mitigation;
- Where some of the services are outsourced to a third party that appropriate reporting and control information is provided to the delegating party by the appointee at regular intervals as defined in the agreement.

Application to In House Teams and Accreditation Approach

The accreditation team will review:

- Evidence of a documented data management policy, to include data security protocols for the transfer of data including evidence of data mapping, risk identification and adoption of procedures to minimise potential risk;
- That a Data Protection Officer has been appointed; if required;
- How the in-house team set the standards and procedures to ensure high quality data standards are achieved;
- Evidence of ongoing training so that employees are aware of the data protection requirements and the implications of not complying;
- Evidence of the data analysis tools used and the results of any reviews undertaken;
- Evidence of systems access limitations, how these are managed and how access rights have been closed down for leavers of where access for an individual is no longer relevant to their role;
- Evidence of appropriate mortality screening and 'living as stated' activity and results;
- Evidence of Fraud risk identification and mitigation;
- Where some of the services are outsourced to a third party that appropriate reporting and control information is provided to the delegating party by the appointee at regular intervals as defined in the agreement.

Application to Master Trusts and Accreditation Approach

The accreditation team will review:

- Evidence of a documented member data management policy, to include data security protocols for the transfer of data;
- How the administration team set the standards and procedures to ensure high quality data standards are achieved;
- Evidence that employees of the Master Trust are aware of the policy and the implications of not complying;
- Evidence of the data analysis tools used and the results of any reviews undertaken;
- Evidence of systems access limitations, how these are managed and how access rights have been closed down for leavers of where access for an individual is no longer relevant to their role;
- Evidence of appropriate mortality screening and ‘living as stated’ activity and results;
- Evidence of Fraud risk identification and mitigation;
- Where some of the services are outsourced to a third party that appropriate reporting and control information is provided to the delegating party by the appointee at regular intervals as defined in the agreement.

Application to Annuity providers and Accreditation Approach

The accreditation team will review:

- Evidence of a documented member data management policy;
- How the administration team set the standards and procedures to ensure high quality data standards are achieved;
- Evidence that employees of the administration provider are aware of the policy and the implications of not complying;
- Evidence of the data analysis tools used and the results of any reviews undertaken;
- Evidence of systems access limitations, how these are managed and how access rights have been closed down for leavers of where access for an individual is no longer relevant to their role;
- Evidence of appropriate mortality screening and ‘living as stated’ activity and results;
- Evidence of Fraud risk identification and mitigation;
- Where some of the services are outsourced to a third party that appropriate reporting and control information is provided to the delegating party by the appointee at regular intervals as defined in the agreement.

Timelines
PASA expects this standard to be applied immediately