Assurity®

Vendor Security Requirements

Ratings	Information Security Control Risk
Low	Handles customer, employee or producer NPPI or HIPAA (cancer policies) **related data less than 250 records annually.**
Medium	Handles customer, employee or producer NPPI or HIPAA (cancer policies) **related data greater than 250 but less than 1,000 records annually.**
High	Handles customer, employee or producer NPPI or HIPAA (cancer policies) **related data greater than 1,000 records annually.**

Low Risk Classification

- Secure computing environment including up to date, active anti-virus / anti-malware software
- Password protected access for all desktop and laptop computers
- Use of encrypted email (e.g. use of Assurity ZixPort) and/or encrypted file transfers for electronic transmission of client NPPI

Medium Risk Classification

- Use of all Low Risk Classification controls specified above
- Completion of all requested due diligence documents including required vendor security questionnaires, and the client NPPI collection and storage forms
- Encryption requirements include:
  - Data encryption for data containing client NPPI, private data, confidential data, financial transactions, identifiers, passwords, etc., during electronic transit (FTP, Web upload, email, etc.)
  - Use of widely accepted, non-deprecated encryption ciphers and algorithms
- Timely periodic security patching performed for all installed computer systems
- Account Management controls for systems with access to NPPI, including:
  - Individually assigned user accounts for all access to client NPPI
  - Secure password policies requiring best practice minimum lengths, complexity, and periodic password change periods
  - Immediate disablement of terminated employee accounts
  - Application of the Principle of Least Privilege for assignment of access rights

High Risk Classification

- Use of all Low and Medium Risk Classification controls specified above
- Documented employee privacy and security policies and security awareness training
- Secure computing environment including:
  - Internal / external firewalls
  - Anti-Virus / Anti-malware installed on all workstations / servers / portable devices
  - Timely vulnerability assessment and patching of operating system and application software vulnerabilities
  - Secure physical facility for server and network infrastructure
  - Periodic third party security assessment testing of external web portals, services and remote access methods
- Encryption requirements include:
  - Storage encryption of all client NPPI on mobile devices including tablet and laptop computers, smart phones, and portable media such as thumb drives, external drives, backup tapes, etc.
  - Data storage encryption for workstations and servers, or well documented alternative protection controls
- A written information security program approved by the vendor's president or board of directors
- Regular testing / auditing of the vendors information security program
- A documented records retention policy or program pertaining to Assurity NPPI
- A documented Incident Response Plan
- A documented Disaster / Recovery Plan
- Ongoing cybersecurity monitoring and logging
- Software development security standards and controls (for vendors and TPSPs that develop or contract development of NPPI application systems)
- Multi-factor authentication (MFA) required for remote access to an environment containing client NPPI over public access networks (i.e. the internet, external Wi-Fi networks, etc.)
- Service Organizational Control audit reports within the past two years for Cloud Providers and Co-location providers where client NPPI is stored or processed