PLANSOURCE®

Technology and Security Overview for 2024

PLANSOURCE

Table of Contents

PLANSOURCE

About PlanSource

- Founded in 2008
- 4 Locations including: Orlando Florida, Salt Lake City Utah, Charleston South Carolina, and Bangalore India
- 850+ Employees
- 500+ Brokers

PlanSource automates and streamlines every aspect of employee benefits programs, so HR teams can spend less time on ben admin tasks and more time where it really matters. Our powerful platform configurability, strong industry partnerships and relentless commitment to creating wildly successful customers are why more than 5,000 employers and 7.5 million consumers trust PlanSource for their benefits.

Security High Level Overview:

PlanSource Benefits is a cloud-based benefit administration system. The PlanSource Platform provides you with numerous efficiencies and helps to deliver a better benefits experience. The Platform acts as a storehouse of data that allows you to easily sort personal information and connect employees to the benefits that are best for them.

The foundation of our security approach is built around ISO 27001 standard. We understand that benefits information is extremely sensitive and have strict procedures and technology safeguards in place to keep it safe. This includes following HIPAA, and state privacy guidelines, as well as leveraging security elements of SANS Top 20 Common Security Controls (CSC).

These include:

- Procedures in place for data protection and confidentiality
    - Access to customer systems, data, and data centers are restricted to authorized personnel
    - Policies and procedures aligned around the ISO 27001 framework
    - HIPAA, GDPR, CCPA and State Privacy guidelines (such as NY-DFS) are met
    - Vendor risk management
- Standards for people and processes
    - Change controls in place
    - Training provided for employees

- Audited security measures for all related equipment and facilities
    - Restricted to authorized personnel
- The use of well-proven software security mechanisms, including:
    - Strong passwords and password requirements
    - Multi-Factor Authentication
    - Single Sign On (SSO)
- Monitoring and testing
    - Security Operations Center with 24/7/365 monitoring
    - Regular Vulnerability and 3rd Party Penetration testing
    - Regular 3rd Party Network testing

Physical Security Overview:

PlanSource provides physical security in our Offices and utilizes the physical security features of the Tier III Data Centers we utilize. PlanSource Office security includes:

- Badges are provided to all employees include picture ID
- Badge card access systems required for entry always includes logging and reporting
- Security Alarms
- Video cameras with digital NVR recording for at least 30 days

AWS, Azure and Tier III Data Center include:

- N+1 Redundancy for Power, Generators, and HVAC
- Access is restricted to authorized personnel
- Access (key card) required for entry always includes logging and reporting, and requires a government-issued photo ID
- Security Alarms as well as Video cameras with digital NVR recording for at least 30 days maintained by the Data Center
- Physical Security guards present 24x7x365 maintained by the Data Centers
- PlanSource servers in the Tier III Data Center reside in locked cage, or locked cabinet. Access to keys is maintained by the Data Center
- Biometric screening, and/or man-trap cage access systems maintained by the Tier III Data Center
- All equipment is inspected prior to admittance to the Tier III Data Center
- No exterior windows on the Tier III Data Center floor
- PlanSource owned equipment removed from Tier III Data Center that may contain customer data (such as HDs, SSDs, etc.) will be disposed of via a 3rd party disposal company providing certification of destruction.
- SSAE-18 audits (HIPAA – PCI – FISMA/NIST)

Network and Internet Security

As a cloud-based technology company, the Internet is a critical resource for us. However, we are always mindful that, while it is an incredible tool for transmitting information, the Internet also has numerous security issues that must be accounted for, and we have built our systems to be protected from threats.

That is why we use:

- Firewalls are configured to allow only authorized application access ports to our DMZ and internal segments.
- Load-balanced web servers utilizing TLS 1.2/1.3 encryption with perfect forward secrecy, encrypting access for all PlanSource Benefits customers
- Standards-based NIST encryption methods (SFTP, SSH, PGP, SSL) and all data transmitted to external carriers, payroll, and business partners
- DLP Policy-based email encryption for regulatory compliance to ensure sensitive data (including personal data) is encrypted during transit
- PHI Data fields in our database is encrypted and data at rest is encrypted on our SAN. Data housed in AWS is also encrypted at rest. We employ encryption using 256-bit AES encryption to prevent unauthorized access.
- Backups are encrypted with 256-bit AES encryption
- Policies require that each employee have a specific user id so that their actions, and the actions of others, including customers can be identified to a specific person
- Logical role-based access control systems built into the software and systems to ensure that company data is separated from each other

Security Monitoring

- PlanSource utilizes a Security Operations Center with an advanced SIEM to log, monitor and provide tier 1 alerting of security events and intrusion attempts. This includes a full logging solution with 3 years of retention
- PlanSource SOC utilizes multiple threat-intelligence feeds to proactively monitor and anticipate future threats
- Web Application Firewall is used to protect applications from OWASP, bot and other attack threats
- Cloud Native application protection (CNAP), Cloud Infrastructure entitlement management (CIEM), Cloud Posture Management monitoring that includes container and micro service based analysis, and notifications.

- IDS/IPS threat analysis system in our next generation firewalls are utilized to protect and mitigate risks of external attack and or abuse
- Secure Web Gateway with policy-based blocking and filtering along with analytics
- Cloud based email security filtering to block phishing and other malicious actions along with account takeover, and email posture management
- We log and records specific actions including (but not limited to): login, logout, security changes, access changes, new employees, terminated employees, communication to and from remote locations (VPN and EDI transmissions)

Virus, Malware, and other protections

- PlanSource laptops, servers all include virus and malware protection from a top tier endpoint detection and response (EDR) vendor. Laptops, USB and other mobile devices are configured to not retain customer data.
- All laptops are whole disk encrypted for protection against theft, or malicious intent
- Web filtering (secure web gateway) is utilized on all workstations to help protect against malicious activity in the internet
- Email is filtered to remove viruses, malware, and SPAM messages
- Hardware no longer in service is sent to a 3rd party disposal company to either permanently delete the data or physically destroy the equipment to prevent unauthorized access.

Vulnerability and Patch Management

- PlanSource utilizes a patch management program for not only Windows, but other application-based patches and upgrades. We also utilize Linux patch management to ensure that our Linux systems are up to date.
- Vulnerability scanning utilizes a best of breed third-party vulnerability management system to check all our servers, workstations, switches, routers, firewalls and other devices for vulnerabilities. In addition, we are also able to test for OWASP and other web-based vulnerabilities in any of our systems.
- PlanSource utilizes a third party to perform several different types of Penetration Testing during a year. These include manual Application Penetration testing and automated Dynamic Code Analysis testing on the Benefits system as well as a third-party Network or systems pen testing.

System and Application Health Monitoring

- PlanSource staff monitors our systems both internally and externally 24x7x365 including alerting staff to issues and incidents. We utilize several types of monitoring and alerting systems.

Maintenance Windows

- Regular outage for IT Infrastructure maintenance occurs the second Saturday of each month, and normally start at 8 am ET, and end prior to 10 am ET. Customer notifications for these outages are typically sent at least two weeks in advance.

Incident response

PlanSource has a cyber security incident response plan and procedure. Core components include:

- Internally investigate the incident to determine the size, scope and if the issue is legitimate
- Individuals assigned to the incident response team will follow the incident response procedure
- PlanSource management will be notified in the event of a breach, or all other material incidents
- Rapid analysis and remediation, and recovery from any incidents
- Process to inform customers of the incident within 48 hours, through our normal communications channels
- Log, document, and report findings and if needed follow applicable laws and regulatory requirements
- Trending and analysis of events and incidents are reviewed to update policies and procedures where appropriate
- Root cause analysis, and lessons learned are reviewed and added to report findings for applicable incidents

Customer Communications

Release Notifications

PlanSource benefits system major releases occur approximately 3 times per year on the night of the 2nd Wednesday of the release month and are posted on our company website (https://releases.plansource.com/). These are usually during the first 3 quarters of each year. These include general overview and specific technical documentation.

Maintenance Notifications

Customer notifications for maintenance outages are typically sent at least two weeks in advance via our normal communications channels. Emergency maintenance notifications are sent out as needed via our normal communications channels. Our typical communications channel is email to the client/broker(s).

- PlanSource SLA is 98% uptime

Event Notifications

Security Incidents, or other compliance notifications are sent out within 48 hours of determination

Secure Software Development

Software Development

PlanSource Benefits is developed in house, using a Secure Software Development model (SSDLC). Elements of this model include:

- Developers work through a process model that is logged, recorded, and reviewed
- We utilize a secure software code check in system to control access to the source code of the system
- Role based access provides check-in, check-out and read access to the source code, and the specific development, and production branches
- Software goes through a testing review through a quality assurance (QA) program to ensure that the resulting product works as expected
- Developers are expected to code to PlanSource coding standards, which includes OWASP, HTML, JavaScript, and Ruby guidelines just to name a few
- All software modifications are reviewed with static code analysis tools, and where needed manually, with respect to PlanSource security requirements
- All known issues are documented, and workarounds are provided, and/or bug fixes created to resolve issues.

Change Management

PlanSource utilizes several internal change management systems that include:

- Development changes including enhancements, bug fixes, and customer requests are logged, recorded, and assigned to specific employees. Software changes are reviewed, and more complex changes are reviewed during regular meetings.
- Deployments of software through our software code check in system follow documented roll-out processes
- System hardware, and system level changes, including network level changes are logged, recorded, and assigned to specific employees. Documentation also must include how to roll back changes if necessary to recover back to a known state

Access Controls

Internal PlanSource Controls

Server, Network and VM Access

PlanSource utilizes industry standard access controls to restrict access to sensitive systems such as servers, network devices, and Virtual Machine infrastructure systems. Firewalls, WAF and IDS/IPS systems are utilized to protect access from the internet to internally hosted systems.

- Internal Network access is segmented using VLANs, and access to file shares are restricted by file level access control roles
- Access to servers is restricted by role-based access to the Information Technology teams
- Administrative access to workstations is restricted by role-based access to the Information Technology teams using an encrypted communications channel (such as SSH)
- Access to network devices is restricted by role-based access to the Networking team, and further requires authentication by a network user account, using an encrypted communication channel (such as SSH, or HTTPS)
- Virtual Machine infrastructure is restricted by role-based access to the Information Technology teams, and further requires authentication by a network user account.
- Remote access requires the use of an Okta two-factor authentication VPN connection using secure encrypted access, on an approved system
- MFA and SSO is used throughout the enterprise for multiple systems utilizing Okta where possible.
- Firewalls are configured so that only specific required ports are opened from the internet to specific DMZ hosted servers.
- Firewalls are monitored 24/7/365 via our third party Security Operations Center (SOC) alerting us to any incidents

Security Reviews

PlanSource conducts internal security reviews comprising the following:

- Vulnerability Scanning is conducted (at least) monthly, for all networked systems including but not limited to routers, switches, firewalls, servers, workstations, and Wi-Fi
- Network Penetration testing is conducted by a third party regularly and includes the same systems as the vulnerability scanning, but also includes application-based testing as well
- Application Penetration testing is conducted by a third party more than once a year (typically every quarter, immediately after major releases) on the PlanSource Benefits system
- Role Recertification is conducted yearly on access rights to ensure that only the appropriate roles are given to employees

Database Access

PlanSource utilizes several different database systems, and access to these systems is restricted to specific groups.

- Internal SQL databases are restricted by role-based access to the Information Technology teams, and selected system developers, and further requires authentication by a network user account
- Benefits MySQL databases are restricted by role-based access to selected Information Technology Staff, and further requires secondary authentication by a network user account, using an encrypted communication channel (such as SSH). In addition, queries to the production database are rejected unless they come from internal specifically defined systems. We do allow specific Quality Assurance analysts, and systems developers to perform queries to a slave system, but that also requires secondary authentication, and is restricted by role, using an encrypted communication channel (such as SSH).

Application Data and File Access

PlanSource requires that access to the Benefits Application, and all other internal systems by PlanSource employees be performed only in the following manners:

- Physically from one of our offices, using an approved workstation
- Remotely using MFA authentication VPN connection using secure encrypted access, using an approved workstation

Access to our internal systems also requires the use of a VPN connection using secure encrypted access, using an approved system.

.

PlanSource Benefits Controls

Logical Access

There are three primary logical groups for customers. Each of these groups is separated by logical access controls built into the application layer. Each group has a set of specific individual roles (RBAC) that provide access to specific portions of the benefits system for their group. Company and/or Broker administrators can customize the roles that are provided to each group within each company.

- Employee Access
- Company Administrator Access
- Broker Administrator Access (where applicable)

Customer Access

PlanSource Customer web-based access is very basic and only requires a modern internet browser.

- All user interfaces are web-browser based.
- The system supports Microsoft Edge as well as current versions of Firefox, Chrome, Edge and Safari.
- No 'fat' client technologies (client-side Java, Silverlight, Flex, Flash, or browser-specific languages or extensions) are used.
- Browser-side code is restricted to HTML (v5), JavaScript, and CSS. Exceptions allowed for widespread video display components.
- All functionality is to be delivered via HTTPS. Intermingled HTTP (whether native or external) is not allowed. PlanSource currently only support TLS 1.2 and 1.3, and modern browsers using secure encryption standards.

Optional Single-Sign On:

PlanSource supports single sign on utilizing the SAML 2.0 standard for communicating identities over the internet, allowing companies to leverage their already existing credentials for access.

Security Features:

Benefits supports several different multi-factor authentication methods including:

- Google Authenticator
- Telephone SMS (PIN)
- Key Fob (YubiKey)
- Email

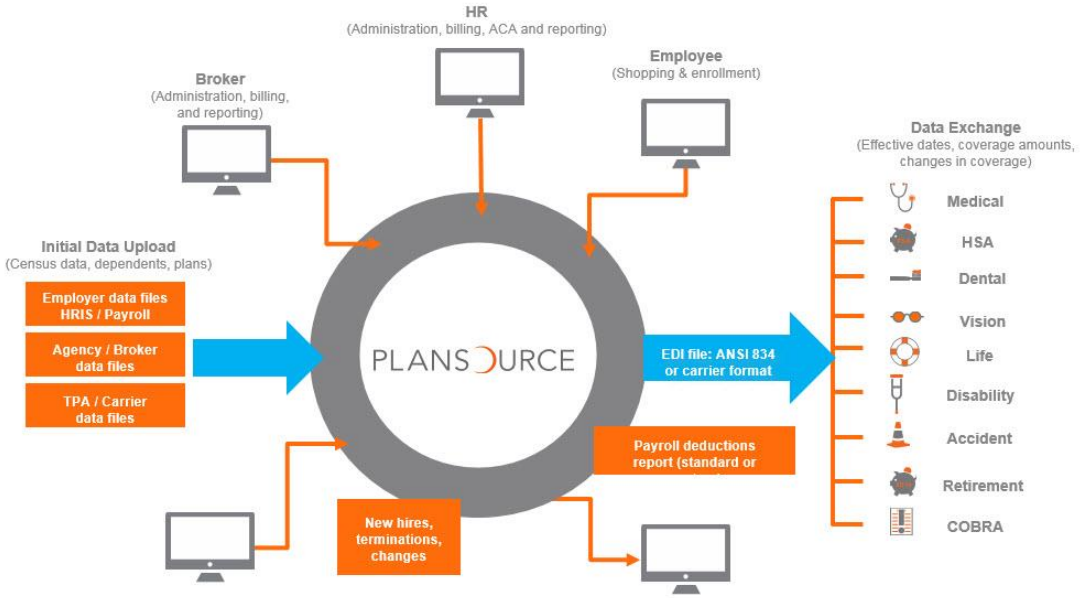
Benefits also supports IP whitelisting to limit administrative access

Secure File Transfers

PlanSource requires by policy that all transfers of customer data over the internet be encrypted using a NIST standard protocol. This includes TLS, SSH, SFTP, FTPS, Email, and/or VPN connections.

Data Flow

PlanSource Benefits as a web-based application provides a portal to your data from a customer perspective, for both the administrators and for the employees. We utilize secure methods to transfer your data to and from your insurance, healthcare, and other service providers. Only the required information is sent to these third parties that you utilize.



Backup and Recovery

Business Continuity, Disaster Recovery, and Business Impact Analysis

We have designed our technology infrastructure to minimize the effects of natural disasters and have business continuity plans in place to ensure that our solutions continue to operate. PlanSource evaluates risk to our business based upon our ISO-27001 framework.

- Disaster Recovery (AWS – Oregon) is kept in a Warm (Passive) state
- All Data Center facilities equipped with redundant power grids, redundant generators, UPSs, and redundant telecommunication trunks.
- Primary Data Center located in Orlando Florida in a Tier III Data Center
- Data is replicated between production and our DR AWS systems have the same data in near real time

- RTO – Recovery time objective of 48 hours
- RPO – Recovery point objective of 4 hours (or less)
- Geographically dispersed HA and Disaster Recovery
    - AWS – Oregon [Disaster Recovery]
    - AWS – Northern Virginia - Analytics [Production]
    - Tier III Data Center – Orlando [Production]
- Established and tested Disaster Recovery and BCP Plans
- Established Customer Communications Plan

Backups

Backups includes multiple types of backup and replication. Frequency includes:

- Replication of data to disaster recovery center in near real time
- Multiple daily backups (approximately every 4 hours), including database backups
- Nightly, Weekly, and Monthly backups (incremental and full)
- Backups are tested for their ability to restore data on a regular basis

Insurance

PlanSource carries Cyber liability insurance in addition to regular business insurance

Risk, Compliance, and Privacy

PlanSource undergoes several audits and reviews each year. These include the SSAE 18 SOC 2 Type 2 audit, a HIPAA Attestation, and a NACHA audit.

ISO 27001 Certification

ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. PlanSource is ISO 27001 certified, and a copy of the current certificate is available upon request.

SSAE SOC 2 Type 2

This is an AICPA (American Institute of CPAs) audit converging the controls a service organization relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy. This is a more stringent report than a SOC 1 which only deals with the Financial Reporting internal controls. Currently this type of audit covers the Trust Service Principle 100 critical controls (COSO controls) of Security, Availability, Processing Integrity, Confidentiality and Privacy. This audit is conducted by a nationally recognized third-party CPA.

Controls tested as part of our SSAE SOC 2 Type 2 audit include:

- Control Environment
- Risk Assessment
- Control Activities
- System Operations
- Risk Mitigation
- Information and Communications
- Monitoring Activities
- Logical and Physical Access Controls
- Change Management

PlanSource provides this report to customers, and their auditors upon request.

HIPAA Assessment

This is an AT-101 type assessment that covers controls and provides proof that PlanSource (acting as a covered entity) is properly securing and safeguarding any ePHI data that it controls. This includes reviewing the following HIPAA rules:

- Security Rule
- Breach Notification Rule
- Privacy Rule, including Administrative, Physical and Technical safeguards

This audit is conducted by a nationally recognized third-party CPA. PlanSource provides this report to customers, and their auditors upon request.

Customer Privacy and Data Retention

PlanSource utilizes the ISO-27001 framework to establish policies that govern the security and privacy of PII and PHI data. PlanSource follows the customer privacy laws set forth in the following (but not limited to) current regulatory requirements:

- Health information Portability and Accountability Act (HIPAA)
- California Consumer Privacy Act (CCPA of 2020)
- US State Privacy laws
- New York Department of Financial Services (NY DFS)
- General Data Protection Regulation (GDPR)
- South Carolina Insurance Data Security Act (2019)
- Colorado Consumer Privacy and Data Protection (2018)
- Massachusetts Data Security Law (updated 2019)

In addition, PlanSource provides customer-based data retention policies and procedures. This allows for the deletion of employee data, and/or customer data on a specific set of schedules. Specifically,

- Disposal of Non-Enrollment Data of data from terminated e recipients of active clients, or terminated clients, 3 years after last business transaction (typically ACA 1095 filing)
- Disposal of Terminated Employees of Active Clients of data from terminated e recipients of active clients, or terminated clients, 3 years after last business transaction (typically ACA 1095 filing)
- Disposal of Terminated Clients
    - Default position, subject to customer approval, is that disposal for terminated clients 3 years after last business transaction (typically ACA 1095 filing)
    - Contract alteration to dispose of data faster is allowed
    - Litigation, or legal hold may suspend disposal

- Certain stored reports (not representing official business transactions) and system tickets to be disposed of within 2 years

Vendor Risk Management

As part of our overall Risk Management program, PlanSource performs vendor risk management reviews.

Information Security:

- PlanSource utilizes ISO-27001 as our template for vendor management
- Vendors are risk tiered based upon a vendor risk-assessment
- Regular reviews (at least annually) are conducted on our vendors based upon risk
- PlanSource captures documentation, and/or certifications (where applicable) such as:
    - ISO-27001 and/or ISO 27018
    - SOC 1, 2 or 3
    - Policies, Procedures, Pen-Testing, Data-Flow Diagrams

Vendor Management Office:

- Business Due Diligence including background screening
- Contractually agreed upon terms (reviewed and approved by our Legal Department)

Security Awareness Training

Security Awareness training covers our policies on information security. In addition, we review several topics on confidential information including HIPAA (PHI) data protections as well as PII security, and privacy. We do our best to ensure that our employees understand privacy requirements, and customer expectations. PlanSource requires all employees (both full, and part time) to complete an Information Security Awareness Training at least yearly. In addition, new hires are required to complete the training within 30 days from their start date.

Awards:

SSAE SOC 2 Type 2:

ISO-27001:

Top Workplace Orlando Sentinel: