Security Overview

Introduction

Security Information overview

This resource provides a synopsis of our retention and administration procedures that secure sensitive data. WEX stores and processes sensitive information. We have privacy and security policies in place for the protection of client data. Each WEX employee acknowledges these policies when he or she is hired, and annually thereafter. WEX considers our policy and procedure documentation proprietary, therefore, within this document we have shared summaries of our practices.

Disclaimer

This resource has been prepared in an effort to highlight key elements of WEX's policies and procedures for review by potential clients, vendors and other third parties. WEX has taken commercially reasonable measures to produce an accurate summary. However, this document is not intended to be a full and complete recitation of WEX's policies and procedures, and the full policies and procedures shall govern.

What we do

WEX provides services as a third-party administrator to assist its clients in administering flexible benefits, COBRA and commuter benefits. The services we offer around benefits include administration of health savings accounts (HSAs), management of health reimbursement arrangements (HRAs), flexible spending accounts (FSAs), commuter benefits, wellness plans, and direct billing services. For a more detailed description of our products and services, please see the WEX Technology Overview in this document.

Who we are

Since 1987, WEX Health Inc. has been simplifying employee benefits administration. We offer cutting-edge technology, instant access to information and expertise, and related customer service.

Financial information, including annual reports, is available under the Investors section of the WEX Inc.'s home page or at SEC.gov – ticker symbol WEX.

The complete web addresses for the preceding links are as follows:

- WEX annual reports page: https://ir.wexinc.com/financials/annual-reports
- WEX Inc.'s home page: https://www.wexinc.com/

WEX Technology Overview

We produce and leverage solutions to solve for the most common industry problems through secure technology that are designed to:

- Give real time visibility into everything you need within our intuitive consumer and client platforms
- Promote automation to ensure data integrity, security, accuracy and transparency
- Allow for agility to quickly adapt to changes and customer needs

Engagement experiences

Our Consumer Engagement Experiences create easy access to reimbursement accounts enabling informed decisions to maximize pre-tax benefits, including online and mobile experiences for account utilization and participation:

- Designed with consumers in mind to deliver a platform that saves time, stress and money.
- Access to all account information in *one* experience is paramount to quickly understand real-time plan details and leverage technology to use benefits.
- Experiences are personalized for consumers based on their level of engagement and needs.

Our COBRA administration includes Consumer Engagement Experiences promote plan compliance and understanding by providing a simple and concise online account and mobile application:

- Qualified beneficiaries need tools that are informative, easy to use and reliable services for when they need it most.
- Designed to reduce confusion for those that need continuation of coverage through COBRA or other alternatives.

Our LEAP™ technology platform provides a guided employer experience through online capabilities, a suite of built-in apps intended to speed up plan setup, offer ongoing account transparency, and provide fast answers to questions:

- Designed with employer, consultants and brokers in mind to deliver a platform that is efficient, user-friendly and saves money.
- The only platform in the industry that provides real-time analytics on ALL administration services to provide transparency and awareness around your plan administration and consumer usage.
- We understand data and providing you with and helping you understand this information is a key driver for a successful partnership together.

Integration tools

Our suite of integration tools offers solutions for the sharing of data that provide a greater level of automation, data integrity, and connectivity to streamline administration. These tools allow us to exchange data with virtually any HR technology partner, health plan and payroll vendor through secure transmission methods.

Account Security with WEX

Account monitoring

Identity Verification (IDV)

We check the identity of every health savings account (HSA) consumer who opens a new account against a national database, per the USA PATRIOT Act. Participants do not have access to funds until they pass IDV, and the account is closed if we are not able to verify the identity of the accountholder.

Enterprise level watch list comparisons

All accounts are compared to an enterprise-level watch list containing demographics of known fraudulent accounts. If we are unable to verify the identity of a consumer, the related account is closed.

New account activity monitoring

We monitor all newly created individual accounts for unusual activity and compare account information to information known to be related to fraudulent accounts.

Bank account activation

All participant-level bank accounts added to the system must pass a bank account activation process to validate the account. If the account isn’t successfully validated, the account cannot be used for contributions or distributions.

Continuous monitoring

Monitoring of consumer account changes and fund requests are performed utilizing technology, data analytics, and manual processes.

Monthly statement distribution

All accountholders have access to monthly account statements so they can monitor activity in their accounts.

Account controls

Account re-opening controls

We do not allow accountholders to re-open a closed account by calling in a request to our Participant Services team — their employer must submit the request and send an updated file.

Account information change controls

Accountholders are not able to change their first or last name through the consumer portal. If changes are made to other accountholder attributes, an email is generated to the accountholder alerting them of the change. We also limit access by user roles internally so only authorized users are able to modify system information.

Account contribution controls

We track all contributions and do not allow contributions in excess of the annual limit for HSAs set by the Internal Revenue Service. We also perform daily reconciliations and closely monitor contributions to verify transaction validity.

Fund access controls

We do not offer participants a credit limit option. Additionally, participants only have access to funds once the deposited funds have been successfully transferred to our custodian. Fraudulent application of funds within the system will not result in fund availability on the participant’s debit card.

Debit card controls

We mail debit cards to accountholders before they have access to account funds, which are not available until the individual logs into their account, accepts the terms and conditions, and completes the IDV process. Our debit card network is restricted to medical, dental, vision and pharmacy expenses only.

Additional precautions

Training

WEX has fraud awareness, privacy and cyber security awareness training programs in place to educate employees about fraud awareness and detection. We also train employees to understand the risks associated with electronic communications, which includes periodic phishing exercises.

Participant identification

Callers are asked additional verification questions to confirm their identity when contacting our Participant Services team. Additionally, when logging into the consumer portal for the first time, consumers must set up security questions. A consumer must answer a security question when requesting an HSA distribution online or resetting their password.

Account alerts

We send notifications to consumers when additional information is needed to open their HSAs. These notifications can be sent if a consumer has not yet accepted their terms and conditions, if they have not yet passed the IDV process or both. These notifications alert consumers about the additional action needed while also serving as fraud protection if a consumer is notified of an action needed on an account they did not initiate.

System Life Cycle Framework

The WEX System Life Cycle (SLC) team follows the Agile Methodology for rapid application development that has as its goal: plan, develop, and deliver in frequent iterative and incremental development cycles. This methodology places a premium on real-time communication and control to deliver custom-developed solutions. Documentation is kept to a minimum, but documented approval cycles are more frequent and rigorous than traditional SLC methodologies.

Four-stage agile SLC

The Portfolio Stage encompasses the initial approval for software changes to WEX Benefits platform. During this phase, enhancement needs and ideas are submitted for additions to the product team from both internal and external sources.

The Sprint Stage encompasses detailed work planning, execution of tasks, demonstrating completed features, and approvals. Business analysts, developers, and quality assurance teams work on features throughout the Sprint.

Release Testing is the point where all features and bug fixes that have made it through the Sprint Stage are subjected to a final level of testing.

The Production Stage is the point where features that have made it through the Release Testing are moved to the production environment. The Release Team formalizes the Release Plan. The Production package is deployed to the Production application and the Production database.

If a release is unsuccessful for any reason, the back-out plan is executed accordingly.

Change Management Summary

WEX's IT change management process balances risks associated with change against organizational risks of not changing. The change control process begins in response to an incident, service request, problem or project. Changes to WEX hardware and infrastructure devices are carried out by WEX IT Infrastructure and performed using a documented process that ensures that requested changes are authorized, developed, tested, approved and implemented in a controlled and consistent manner. Changes are classified as either Standard, Normal, Expedited Normal or Emergency and go through our Change Advisory Board (CAB).

Patch and update management

Patch management is employed to eliminate security vulnerabilities, fix bugs, and enhance the overall performance of systems. Once the need for a patch has been identified, WEX performs an appropriate assessment to evaluate the impact.

Patches may also be installed on software that may be loaded on a system but is currently inactive. For available patches that are not applied, the reason for non-application must be documented. Emergency patches released may be tested and installed outside of the normal patch cycle based on need and possible impact.

Business Resilience

Overview

WEX maintains a Business Resilience Program to mitigate the risk of material losses and business disruptions. The program provides a structure, controls and decision-making protocols to support business continuity in the event of a significant business disruption. The program is designed to provide centralized oversight and governance while enabling business ownership.

Business Resilience is defined as the ability of an organization's business operations to withstand or rapidly adapt and respond to internal and external dynamic changes, including, but not limited to, disruptions or threats, and to continue operations with limited impact to the business.

While it cannot be guaranteed that systems will always be available or recoverable, or that business interruptions will not ensue after a significant event, WEX's business resilience strategy supports our preparedness and provides reasonable assurance that the company can recover from emergencies and disasters.

Business continuity

The foundation of WEX's resilience program is its Business Continuity Plans. Business Areas are required to create and maintain written business continuity plans to safeguard personnel, critical business operations, information technology and facilities.

Business Continuity Plans (BCP) identify core functions, establish the appropriate level of business controls and functionality necessary to mitigate risks, document functional requirements and account for dependencies.

Disaster recovery

In the event of a catastrophe which results in a significant disruption in service, restoring technology supporting critical business process within acceptable timeframes becomes a top priority. Disaster Recovery Plans (DRP) are plans that address the recovery of technology that supports critical business processes.

Incident Management Summary

WEX has well-defined and systematic procedures to respond to security and privacy related events. This ensures WEX is adequately prepared to respond and recover from incidents that may compromise the confidentiality, availability, or integrity of information assets or WEX customer information.

We will cooperate with Federal or State law enforcement through WEX corporate counsel and our Privacy Officer. Standards are in place to provide for initial and ongoing notification to any affected as well as required legal authorities and the public, as appropriate.

The WEX incident response framework includes seven phases that ensure a consistent and systematic approach: Preparation, detection, containment, investigation, remediation/recovery, root cause analysis, long-term remediation/response review.

Vendor Management Overview

WEX uses a rigorous vendor selection and management process to oversee the relationship, quality, and security of vendor resources. The management processes have some variation, dependent on the type of relationship and tasks that the vendor handles. The program components include an annual assessment, employee onboarding requirements and periodic review of access.

Vendors are assigned a risk ranking according to a set of classification standards and questions answered by the Information Security team during the vendor review process. Additional research for information regarding the vendor to identify any additional risks is performed. Critical vendors undergo annual assessments that are reviewed by the Information Security team and submit to independent assessments of their security.

All contracts cover confidentiality, privacy and security obligations, as applicable, for the services being agreed to. Ongoing monitoring is completed of the vendor’s performance.

Written Information Security Program

The objective of WEX, in the development and implementation of this comprehensive written information security program (WISP), is to create effective administrative, technical, and physical safeguards for the protection of sensitive information. The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, processing, transmitting, and protecting sensitive information.

Purpose

The WISP is designed to establish a system of controls to protect the confidentiality, availability, and integrity of sensitive information WEX is the owner or custodian of. The WISP is designed to protect all sensitive information including personal information, which is of special interest to WEX Partners and Clients.

Therefore, while the WISP covers all sensitive information, this security overview will primarily focus on personal information.

The WISP defines “personal information” as defined as the first name and last name or first initial and last name in combination with any one or more of the following:

a) Social Security number.

b) Driver's license number or state-issued identification card number.

c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a person’s financial account.

Personal information does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Additionally, WEX possesses and uses a variety of sensitive information, much of which may not be directly covered by the provisions of this program. Some information is covered by other state, federal, or industry regulations under which we are required to comply, such as the Health Insurance Portability and Accountability Act (HIPAA). Other information may be protected by contractual commitments undertaken by WEX.

Scope

The WISP applies to all WEX employees and certain contracted third-party vendors. The data covered by this program includes any information stored, accessed, processed or collected at WEX for the purposes of administrating benefits or COBRA for our clients. The WISP is not intended to supersede any existing WEX policy that contains more specific requirements for safeguarding data. If such policy exists and is in conflict with the requirements of the WISP, the other policy takes precedence.

In formulating and implementing the WISP, WEX has addressed and incorporated the following protocols:

1. Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information.
2. Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information.
3. Evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.
4. Designed and implemented a WISP that puts safeguards in place to minimize those risks.
5. Implemented regular monitoring of the effectiveness of those safeguards.

Protection of personal information

WEX's Chief Information Security Officer is responsible for implementing, supervising, and maintaining the WISP, along with the following:

- Implementation of the WISP including all provisions outlined in the policies section.
- Regular testing of the WISP's safeguards.
- In coordination with the WEX Health Privacy Officer, evaluating the ability of any of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third-party service providers by contract to implement and maintain appropriate security measures.
- Reviewing the scope of the security measures in the WISP annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.
- Assist in ensuring the annual employee and new hire training sessions required for all employees and new hires coordinated through our training department are completed. All attendees are required to certify their attendance at the training, and their familiarity with the requirements for ensuring the protection of personal information**.**

Risk identification and assessment

WEX recognizes that we have both internal and external risks to the privacy and integrity of personal information. These risks include but are not limited to:

- Unauthorized access of personal information, including unauthorized requests, access through hard copies or reports, unauthorized transfer through third parties
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission

- Loss of data integrity
- Loss of data from physical disaster, corruption of data or systems or errors introduced to the system

WEX's Enterprise Risk Management Team actively monitors new risks by conducting regular risk assessments and considers threat issues/changes from US-CERT and other related entities.

Policies and practices for safeguarding personal information

To guard against internal risks to the security, confidentiality, and/or integrity of personal information the following policies are in place:

Organization of Information Security

Global Information Security Policy
Mobile Device Security Policy

Human Resources Security

Global Information Security Awareness & Training Policy

Asset Management

Acceptable Use Policy
Global Data Leak Prevention Policy
Global Configuration Management P
Global Information Classification and Handling Policy

Access Control

Global Access Control and Password Policy

Cryptography

Global Encryption and Key Management Policy

Physical and Environmental Security

Global Equipment Disposal Policy
Physical Security and Access Policy

Operations Security

Change Management Policy
Global Virus Protection Policy
Global Cloud Security Policy
Global Data Backup Policy
Global Event Logging and Monitoring Policy
Global Patch Management Policy
Global Vulnerability Management Policy

Communications Security

Global Network Security Policy

Systems Acquisition, Development and Maintenance

Systems Development Life Cycle Methodology Policy
Global Secure Coding and Code Review Policy

Supplier Relationships

Information Security Third Party Diligence Policy
Vendor Management Policy

Information Security Incident Management

Global Information Security Incident Response Policy
Cyber Forensics Policy

Information Security Aspects of Business Continuity Management

Business Continuity Policy

Compliance

Global Record Management Policy
Record Retention and Destruction Policy

Review and modifications to the program

All security measures, including the WISP, are reviewed at least annually to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations.

If our business practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information, the WISP is reviewed to ensure that the policies contained in the WISP are adequate to meet all applicable federal and state regulations.

The Security Officer and Privacy Officer are responsible for all review and modifications of the security policies including the WISP and will fully consult and apprise management of all reviews including any recommendations for improved security arising from the review.