



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

Nevada Health Authority
Division of Consumer Health Services
Silver State Health Insurance Exchange
Nevada Health Link

Rules of Behavior for Exchange Enrollment Facilitators

Version	Issue Date	Changes	Drafted	Approved	Next Review
26.01	September 1, 2026	Initial Release	J. Filippi	S. Moses	August 2027

Table of Contents

1. Purpose and Applicability	2
2. User Acknowledgment – Conditions of Access	2
2.1 Authorized Use Requirements	3
2.2 Privacy and Security Standards	3
2.3 Penalties for Misuse of Information	3
3. User Responsibilities	4
3.1 Consumer Assistance Responsibilities	5
3.2 Prohibited Activities/Conflicts of Interest	7
4. Acknowledgment Signature	10



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

1. Purpose and Applicability

The Nevada Health Link Rules of Behavior outline role-specific responsibilities of Exchange Enrollment Facilitators (EEFs), including Certified Application Counselors (CACs) and Navigators. In Nevada, in addition to federal regulatory requirements, enrollment assisters such as CACs and Navigators are required to hold an Exchange Enrollment Facilitator (EEF) certification issued by the Nevada Division of Insurance and comply with provisions of N.R.S. Chapter 695J and N.A.C. Chapter 695J.

As an Exchange Enrollment Facilitator and a Nevada Health Link (Nevada Health Link) Health Insurance Exchange User (**User**), you must understand and agree to these Rules of Behavior and Acceptable Use Agreement prior to being granted access to the Nevada Health Link system to perform enrollment activities authorized under the Patient Protection and Affordable Care Act (ACA) for the Nevada Health Insurance State-Based Exchange, Nevada Health Link.

By signing this form, you, the User, affirm your knowledge and understanding of, and agreement to adhere to, the Nevada Health Link Rules of Behavior and the Silver State Health Insurance Exchange Acceptable Use Agreement.

As outlined in the Acceptable Use Agreement, Nevada Health Link Information Resources include, but are not limited to, applications, systems, files, documents, spreadsheets, databases, data, software, software code, user/login ids and passwords, electronic mail, Personally Identifiable Information (**PII**), Protected Health Information (**PHI**), Federal Tax Information (**FTI**), confidential or other sensitive information, State and Federal records and Nevada Health Link equipment.

Where these rules do not provide explicit guidance, Users are encouraged to apply best judgment based on the principles stated here and in applicable law or consult the Nevada Health Link team at privacy@nvha.nv.gov.

Non-compliance may result in administrative, civil, or criminal actions, including:

- Suspension of access privileges;
- Revocation of access to certain information, information systems, and/or facilities;
- Report to licensing entity or another agency;
- Termination of role with Nevada Health Link;
- Removal or disbarment from work in certain areas or projects;
- Monetary fines; and/or
- Criminal charges that may result in fines or imprisonment.

2. User Acknowledgment – Conditions of Access

EEF Users of Nevada Health Link Information Resources must acknowledge the following statements:

2.1 Authorized Use Requirements

I affirm my understanding that:

- a) For Certified Application Counselors: I may only use Nevada Health Link Information Resources consistent with 45 C.F.R. 155.225 entitled “Certified application counselors” and my Certified Application Counselor Designated Organization’s agreement with Nevada Health Link;
- b) For Navigators: I may only use Nevada Health Link Information Resources consistent with--
 - a. 45 C.F.R. 155.210 “Navigator program standards,” and 45 C.F.R. 155.215 “Standards applicable to Navigators...carrying out consumer assistance functions...”; and
 - b. my Navigator entity’s agreement with Nevada Health Link.
- c) As an Exchange Enrollment Facilitator, I may only use Nevada Health Link Information Resources consistent with N.R.S. Chapter 695J entitled “Persons Who Facilitate Enrollment in Certain Qualified Health Plans” and consistent with N.R.S. Chapter 422 entitled “Medicaid and Other Health Care Programs”; as well as any policies established by the Nevada Health Authority, Nevada Health Link and Nevada Medicaid.

2.2 Privacy and Security Standards

Use of Nevada Health Link Information Resources must be in compliance with the **Silver State Health Insurance Exchange Acceptable Use Agreement** and federal ACA privacy and security regulations outlined in 45 C.F.R. 155.260. Use of Nevada Health Link Information Resources is limited strictly to authorized Certified Application Counselor or Navigator duties and permitted by the ACA and other applicable laws. Unauthorized use is a privacy/security violation and subject to penalty.

2.3 Penalties for Misuse of Information

- Knowing/willful uses or disclosures of Nevada Health Link PII in violation of the ACA subjects the user or entity to a civil monetary penalty of not more than \$25,000 (adjusted annually) per use or disclosure in addition to other penalties prescribed by law (45 C.F.R. 155.285);
- Under the ACA, any person who, with negligence and disregard, fails to provide correct application information to Nevada Health Link may be subject to a maximum civil money penalty of \$25,000 for each application (45 C.F.R. 155.285(c)(1)(i)); and;
- Under the ACA, any person who knowingly and willfully provides false or fraudulent application information to Nevada Health Link may be subject to a maximum civil money penalty of up to \$250,000 for each application (45 C.F.R. 155.285(c)(1)(ii)).

3. User Responsibilities

Users must:

- **Comply with applicable federal and State statutes and regulations for assisting consumers on the Nevada Health Link platform**, including, as appropriate, for Certified Application Counselors - 45 C.F.R. 155.225 entitled “Certified Application Counselors;” or for Navigators - 45 C.F.R. 155.210 “Navigator program standards,” 45 CFR 155.215 “Standards applicable to Navigators...carrying out consumer assistance functions...,”; and Exchange Enrollment Facilitators – N.R.S. and N.A.C. Chapter 695J “Persons Who Facilitate Enrollment in Certain Qualified Health Plans”.
- Maintain the privacy and confidentiality of all Nevada Health Link consumer information, PII, PHI, FTI, confidential information or other sensitive information as required by –
 - The Silver State Health Insurance Exchange Acceptable Use Agreement
 - the Patient Protection and Affordable Care Act (PPACA) (45 C.F.R. 155.260),
 - the Health Insurance Portability and Accountability Act (HIPAA) (45 C.F.R. 160 and 164),
 - the Internal Revenue Code, 26 U.S.C. 6103, regarding FTI,
 - other relevant laws as determined by the state, including those governing the Nevada Medicaid program—
 - the Medicaid Act (42 C.F.R. 431.300) and
 - the Children’s Health Insurance Program (CHIP) (42 C.F.R. 457.1110 regarding safeguarding sensitive information);

Before accessing any Nevada Health Link Information Resources Users must:

- Obtain active certification as an Exchange Enrollment Facilitator (EEF) with the Nevada Division of Insurance and achieve a passing score on all mandatory annual Nevada Health Link Certified Assister training regarding qualified health plan options, insurance affordability programs, eligibility rules and regulations governing insurance affordability programs operated in the State, the needs of underserved and vulnerable populations, and privacy and security standards;
- Maintain active EEF license issued by Nevada Division of Insurance and associated requirements;
- Maintain Nevada Health Link certification requirements;
- Complete Nevada Health Link certification/re-certification at least annually

-
- Users must cooperate with audits, monitoring, compliance reviews, and program oversight activities conducted by Nevada Health Link.

3.1 Consumer Assistance Responsibilities

- Prior to providing assistance and accessing consumer PII, provide a statement to consumers of the functions and responsibilities of, as appropriate, Certified Application Counselors or Navigators, the items of information about the consumer that will be collected, what the consumer's information will be used for, and where it will be maintained.
- Users must abide by all applicable federal or state laws and regulations, including 45 CFR § 155.260 as it pertains to the privacy and security of PII. Assisters must continue to protect any PII accessed during the term of this Agreement with the Exchange. All PII in the possession of the Assister must be retained and destroyed in accordance with the record retention period. The duty of Assisters is to protect and maintain the privacy and security of PII, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.
- *Prior to providing assistance*, advise consumers that, as appropriate, Certified Application Counselors or Navigators are not tax advisors or attorneys and cannot provide tax or legal advice within their capacity as an assister; and disclose any other information required by law;
- **For Certified Application Counselors**, disclose any relationships that I or my sponsoring agency have with qualified health plans, insurance companies/carriers, insurance agents or brokers, insurance affordability programs, or other potential conflicts of interest;
- For all assisters, ***prior to assisting with an application or enrollment*** and after providing a Privacy Notice statement, **obtain written or documented consumer consent/authorization in hard copy or electronic format**. The consent should advise that it can be revoked at any time. A record of this consent should be kept for ten years;¹
 - 1) Only personnel who need to access the consent/authorization records to carry out their duties and responsibilities should be given access to them;
 - 2) Hard copies must be kept in a secure location, locked and with limited access save for authorized individuals;
 - 3) Electronic copies must be kept as a password-protected file that is kept securely at all times. Files must be maintained only in Nevada Health Link-approved systems or storage locations that are subject to established security and record-management controls.

¹ If you or your organization is required under federal law to maintain a record of authorization for a period that is longer than ten years, the longer retention period must be followed.

-
- Assist individuals to apply for coverage in a qualified health plan or for insurance affordability programs (such as Nevada Medicaid) through Nevada Health Link and help to facilitate enrollment of eligible individuals in qualified health plans or insurance affordability programs.
 - Provide consumers with correct information, without omission of material fact, regarding Nevada Health Link and the full range of qualified health plan options and insurance affordability programs (such as Nevada Medicaid and Nevada Check Up programs) for which a consumer may be eligible, which includes: providing fair, impartial, and accurate information that assists consumers with submitting the eligibility application; clarifying the distinctions among health coverage options, including qualified health plans; and helping consumers make informed decisions during the health coverage selection process.
 - **For all EEFs**, maintain expertise in eligibility, enrollment, and program specifications, and facilitate selection of health plans that best serve the consumer's insurance needs and interests (NRS 695J.220).
 - Provide information and services in a fair, accurate, and impartial manner, which includes providing information that assists consumers with submitting the eligibility application; clarifying the distinctions among health coverage options, including QHPs; and helping consumers make informed decisions during the health coverage selection process. Such information must be acknowledged by other health programs.
 - Provide referrals to the Division of Insurance, Division of Nevada Medicaid, Division of Consumer Health Services, Division of Social Services or other appropriate State agencies, for any enrollee with a grievance, complaint, or question regarding their health plan, coverage, or a determination under such plan or coverage.
 - Provide information in a manner that is culturally and linguistically appropriate to the needs of the population being served by Nevada Health Link, including individuals with limited English proficiency.
 - Provide consumers with information and assistance in the consumer's preferred language, at no cost to the consumer, including the provision of oral interpretation of non-English languages and the translation of written documents into non-English languages when necessary or when requested by the consumer to ensure effective communication. Use of a consumer's family or friends as oral interpreters can satisfy the requirement to provide linguistically appropriate services only when requested by the consumer as the preferred alternative to an offer of other interpretive services.
 - Provide oral and written notice to consumers with limited English proficiency, in their preferred language, informing them of their right to receive language assistance services and how to obtain them.

-
- Provide auxiliary aids and services for individuals with disabilities, at no cost, when necessary or when requested by the consumer to ensure effective communication. Use of a consumer's family or friends as interpreters can satisfy the requirement to provide auxiliary aid and services only when requested by the consumer as the preferred alternative to an offer of other auxiliary aid and services.
 - Be able to work with all individuals regardless of age, disability, or culture, and seek advice of experts when needed. Acquire sufficient knowledge to be able to refer people with disabilities to long-term services and supports programs when appropriate. Ensure authorized representatives are permitted to assist an individual with a disability to make informed decisions. Provide assistance to consumers in a location and in a manner that is physically and otherwise accessible to individuals with disabilities.
 - Refrain from conduct that discriminates based on race, color, national origin, disability, age, or sex. Refraining from discrimination includes refraining from discrimination based on sexual orientation, gender identity, on the basis of sex stereotypes, sex characteristics including intersex traits, and pregnancy or related conditions.
 - **For Certified Application Counselors**, either directly or through an appropriate referral, provide information in a manner that is accessible to individuals with disabilities, as defined by the Americans with Disabilities Act, as amended, 42 U.S.C. 12101 et seq. and section 504 of the Rehabilitation Act, as amended, 29 U.S.C. 794.
 - **For Navigators**, in addition to the above, ensure accessibility and usability of Navigator tools and functions for individuals with disabilities in accordance with the Americans with Disabilities Act and section 504 of the Rehabilitation Act.

3.2 Prohibited Activities/Conflicts of Interest

As outlined in NRS 695J.210, Exchange Enrollment Facilitators (EEFs) **must not**:

- Hold a license as a producer of insurance, an insurance consultant or broker;
- Sell, solicit, or negotiate insurance;
- Accept any payment (directly or indirectly) from health insurance issuers or stop-loss insurance issuers relating to enrollments in qualified health plans;
- Employ, be employed by, partner with, or receive payment stemming from their facilitator role from:
 - Licensed insurance producers,
 - Insurance consultants,
 - Surplus lines brokers, or
 - Insurers

In addition, all assisters must remain free from conflicts of interest in serving Nevada Health Link consumers.

For Navigators, remain free of conflicts of interest including that a Navigator (and their staff) **must not**:

- 1) Be a health insurance company or issuer of stop loss insurance;
- 2) Be a subsidiary of a health insurance company or issuer of stop loss insurance;
- 3) Be an association that includes members of, or lobbies on behalf of, the insurance industry;
- 4) Receive any consideration directly or indirectly from any health insurance company or issuer of stop loss insurance in connection with the enrollment of any individuals in a qualified health plan (QHP) or a non-QHP;
- 5) Charge any applicant or enrollee, or request or receive any form of remuneration from or on behalf of an individual applicant or enrollee, for application or other assistance related to Navigator duties;
- 6) Provide an applicant or potential enrollee gifts of any value as an inducement for enrollment. The value of gifts provided to applicants and potential enrollees for purposes other than as an inducement for enrollment must not exceed nominal value, either individually or in the aggregate, when provided to that individual during a single encounter. For purposes of this paragraph, the term gifts includes gift items, gift cards, cash cards, cash, and promotional items that market or promote the products or services of a third party, but does not include the reimbursement of legitimate expenses incurred by a consumer in an effort to receive Exchange application assistance, such as travel or postage expenses.
- 7) Use Exchange funds to purchase gifts or gift cards, or promotional items that market or promote the products or services of a third party, that would be provided to any applicant or potential enrollee;

For Certified Application Counselors, comply with federal fee, consideration, solicitation and marketing requirements for Certified Application Counselors set forth at 45 CFR 155.225(g) including compliance with the following: Certified Application Counselors and their Designated Organizations **must not**—

- (1) impose any charge on applicants or enrollees for application or other assistance related to Nevada Health Link;
- (2) receive any consideration, such as gifts, rebates, vacations, or prizes, directly or indirectly from any health insurance company or any company providing stop-loss insurance in connection with the enrollment of any individual in a qualified health plan or a non-qualified health plan;
- (3) provide compensation to individual Certified Application Counselors on a per-application, per-individual-assisted, or per-enrollment basis;
- (4) provide to an applicant or potential enrollee gifts of any value as an inducement for enrollment. The value of gifts provided to applicants and potential enrollees for purposes other than as an inducement for enrollment must not exceed nominal value, either individually or in the aggregate, when provided to that individual during a single encounter;
- (5) Solicit any consumer for application or enrollment assistance by going door-to-door or through other unsolicited means of direct contact, including calling a consumer to provide application or enrollment assistance without the consumer initiating the contact, unless the individual has



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

-
- a pre-existing relationship with the individual Certified Application Counselor or Designated Organization and other applicable State and Federal laws are otherwise complied with. Outreach and education activities may be conducted by going door-to-door or through other unsolicited means of direct contact, including calling a consumer; or
- (6) Initiate any telephone call to a consumer using an automatic telephone dialing system or an artificial or prerecorded voice, except in cases where the individual Certified Application Counselor or Designated Organization has a relationship with the consumer and so long as other applicable State and Federal laws are otherwise complied with.

[signature on next page]



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

4. Acknowledgment Signature

By signing this form, you, the User, affirm you have received, reviewed, and agree to comply with both the Rules of Behavior and the SSHIX Acceptable Use Agreement.

I, the User, have read the Nevada Health Link Rules of Behavior and the SSHIX Acceptable Use Agreement of Information Resources and understand and agree to comply with its provisions. I understand that violations may result in administrative, civil, or criminal action, including termination of access, removal from projects, revocation of system/facility access, licensing penalties, civil penalties, or imprisonment. I understand that exceptions must be authorized in writing by the Nevada Health Link security team. I also understand certain privacy law violations carry monetary and criminal penalties.

NAME (PRINT)	
SIGNATURE	
EMPLOYER (LEGAL NAME)	
DATE	



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

Silver State Health Insurance Exchange (SSHIX) Acceptable Use Agreement

August 27, 2026

Version 26.01



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

Table of Contents

1. Purpose.....	3
2. Requirements.....	3
2.1 Authorized Access and Account Security.....	3
2.2 Protection of SSHIX Systems and Information.....	4
2.3 Devices Used to Access SSHIX Resources.....	4
2.4 Software and Technology.....	4
2.5 Storage and Transmission of Sensitive Data	5
2.6 Federal Tax Information	5
2.7 Workstation, Session, and Physical Security	5
2.8 Records and Data Retention	6
2.9 Security and Privacy Incident Reporting.....	6
2.10 Termination or Change of Access	6
3. Prohibited Actions	7
3.1 Unauthorized Access and Credential Use.....	7
3.2 Unauthorized Devices, Software, and Services	7
3.3 Protection and Handling of Sensitive Data	8
3.4 Electronic Communications	8
3.5 Internet and External Service Use.....	9
3.6 Personal Use.....	9
3.7 Security and Privacy Violations	9
4. Complaints	10
5. Consequences	10
6. Definitions.....	10
7. Document Revision History	12

Purpose

This acceptable use agreement governs the use of computers, networks, and other information technology (IT) resources administered by the Silver State Health Insurance Exchange (SSHIX), including the Nevada Health Link SBE Platform (SBE Platform). This statement applies to all SSHIX employees and contractors, insurance carrier personnel utilizing the SBE Platform for Plan Management or Enrollment Reconciliation functions, and any other persons authorized to access or use SSHIX systems, resources, or information owned or managed by SSHIX, including devices connected by any means to Nevada's SilverNet Wide Area Network.

IT resources within SSHIX shall be used only in a manner consistent with authorized business purposes. "IT resources" include State- or SSHIX-owned or managed hardware, software, computers, mobile devices, networks, applications, cloud services, information systems, and data, as well as personally owned or third-party devices used to access SSHIX systems or information.

Requirements

Users of SSHIX systems, information, networks, applications, devices, and other IT resources are responsible for protecting the confidentiality, integrity, and availability of those resources and for using them only for authorized business purposes.

2.1 Authorized Access and Account Security

Users shall:

- Access only those systems, applications, functions, and information for which they have been specifically authorized.
- Use SSHIX access only for legitimate business purposes consistent with the user's assigned duties or authorized functions.
- Protect passwords, access codes, authentication tokens, certificates, multifactor authentication methods, and other authentication credentials from unauthorized use or disclosure.
- Maintain unique user accountability and shall not share accounts or credentials with another individual.
- Comply with authentication and access-control requirements established by SSHIX, NVHA, or the State of Nevada, including multifactor authentication where required.
- Promptly report suspected credential compromise, unauthorized account activity, or other indications that an account may have been misused.
- Comply with access restrictions and shall not attempt to circumvent, disable, or bypass security controls.

Access privileges shall be limited to the minimum level necessary to perform the user's authorized functions.

2.2 Protection of SSHIX Systems and Information

Users shall safeguard SSHIX systems and information against unauthorized access, use, disclosure, alteration, destruction, loss, or disruption.

Users shall:

- Access, use, modify, transmit, disclose, retain, or dispose of information only when authorized.
- Access and use only the minimum information reasonably necessary to perform the user's authorized function.
- Introduce or enter information into SSHIX systems only when it serves a legitimate and authorized business purpose.
- Protect nonpublic and Sensitive Data when stored, processed, displayed, printed, or transmitted.
- Follow applicable federal, State of Nevada, NVHA, and SSHIX privacy, security, records-management, and information-handling requirements.
- Protect SSHIX information from unauthorized disclosure when communicating over internal or external networks.

2.3 Devices Used to Access SSHIX Resources

State-owned, SSHIX-managed, personally owned, or third-party devices may be used to access SSHIX systems or information only when such access is authorized.

Devices used for authorized access shall:

- Be protected against unauthorized physical and logical access.
- Use appropriate device authentication and access controls.
- Maintain current security updates and supported software where applicable.
- Use malware protection or other endpoint safeguards where required.
- Use encryption where required based on the type or sensitivity of information being accessed or stored.
- Comply with applicable SSHIX, NVHA, and State of Nevada device-security requirements.

Users shall not download, locally store, copy, or otherwise retain SSHIX Sensitive Data on personally owned or unauthorized devices unless specifically authorized.

Users shall immediately report the loss, theft, compromise, or suspected compromise of any device containing SSHIX information or used to access SSHIX systems.

2.4 Software and Technology

Only authorized and properly licensed software, applications, browser extensions, utilities, and other technology may be installed or used on SSHIX-managed devices or systems.

Users shall:

- Comply with applicable software licensing requirements.

-
- Use software and technology only for authorized purposes.
 - Obtain required approval before installing software or connecting devices to SSHIX-managed systems or networks.
 - Not use software, services, or technology designed or configured to circumvent established security controls.

2.5 Storage and Transmission of Sensitive Data

SSHIX Sensitive Data shall be stored, processed, and transmitted only through systems, applications, and methods authorized for the sensitivity and classification of the information.

Users shall:

- Use approved secure transmission methods when transmitting PII, PHI, financial information, or other Sensitive Data.
- Apply encryption where required by applicable law, regulation, policy, agreement, or data classification.
- Verify recipients and transmission methods before sending Sensitive Data.
- Limit Sensitive Data included in communications to the minimum information necessary for the authorized business purpose.
- Not transmitting or storing Sensitive Data through personal email, personal cloud storage, unauthorized file-sharing services, unauthorized messaging platforms, artificial intelligence services, or other unapproved systems.

2.6 Federal Tax Information

Users authorized to access Federal Tax Information (FTI) shall safeguard such information at rest and in transit in accordance with applicable requirements of IRS Publication 1075 and SSHIX-approved FTI security policies, standards, and procedures. FTI shall be accessed, used, disclosed, stored, and transmitted only for authorized purposes and only by individuals authorized to receive such information. Transmission of IRS Forms 1095-A or any other information constituting FTI through email, fax, or any other method prohibited by applicable IRS requirements or SSHIX policy is prohibited.

2.7 Workstation, Session, and Physical Security

Users shall take reasonable precautions to prevent unauthorized persons from accessing or viewing SSHIX systems or Sensitive Data.

Users shall:

- Lock or otherwise secure workstations and devices when left unattended.
- Prevent unauthorized persons from viewing Sensitive Data displayed on screens or printed materials.
- Secure printed or physical records containing Sensitive Data when not in use.
- Dispose of Sensitive Data only through authorized secure-disposal methods.
- Take appropriate precautions when accessing SSHIX systems from remote, public, or shared locations.

2.8 Records and Data Retention

SSHIX information shall be retained and disposed of in accordance with applicable records-retention requirements and authorized business processes.

Users shall not:

- Retain SSHIX information longer than authorized or required.
- Create unnecessary duplicate copies of Sensitive Data.
- Destroy, alter, conceal, or dispose of records in violation of applicable retention requirements, legal holds, investigations, audits, or other preservation obligations.

2.9 Security and Privacy Incident Reporting

Users shall promptly report suspected or actual security or privacy events involving SSHIX systems or information, including but not limited to:

- Unauthorized access or disclosure.
- Suspected credential compromise.
- Phishing or other suspected social-engineering activity affecting SSHIX access.
- Malware or other malicious activities.
- Loss or theft of devices or information.
- Unintended delivery or transmission of Sensitive Data.
- Suspected misuse of SSHIX systems or information.
- Attempts to circumvent security controls.
- Any other event that may compromise the confidentiality, integrity, or availability of SSHIX systems or information.

Reports shall be made through the reporting process established by SSHIX. Users shall not include passwords, authentication credentials, FTI, or unnecessary PII or PHI in an initial email notification.

Users shall cooperate with SSHIX, NVHA Information Security, Privacy, and other authorized personnel in the investigation, containment, remediation, recovery, and documentation of security or privacy events.

2.10 Termination or Change of Access

When a user's employment, contract, business relationship, or authorized function ends or changes, the user shall no longer access SSHIX systems, accounts, information, or privileges for which authorization no longer exists.

Users shall return or appropriately dispose of SSHIX-owned or SSHIX-provided equipment, information, software, records, and other resources as directed.

Users shall not retain copies of SSHIX information following termination of authorized access unless specifically permitted by applicable law, agreement, or written authorization.

Prohibited Actions

Users shall not use SSHIX systems, information, networks, applications, devices, or other IT resources in a manner that is unlawful, unauthorized, inconsistent with legitimate business purposes, or that could adversely affect the confidentiality, integrity, or availability of SSHIX systems or information.

Prohibited activities include, but are not limited to, the following:

3.1 Unauthorized Access and Credential Use

Users shall not:

- Access or attempt to access systems, applications, information, functions, or privileges for which they have not been specifically authorized.
- Use another individual's account, credentials, authentication token, certificate, or other means of authentication.
- Share passwords, authentication tokens, multifactor authentication approvals, access codes, or other authentication credentials with another individual.
- Permit another person to use an account or system session assigned to the user.
- Attempt to obtain elevated privileges or otherwise exceed assigned access permissions without authorization.
- Circumvent, disable, modify, interfere with, or attempt to bypass security controls, access restrictions, monitoring, logging, endpoint protection, encryption, or other safeguards implemented by SSHIX, NVHA, or the State of Nevada.

3.2 Unauthorized Devices, Software, and Services

Users shall not:

- Connect unauthorized hardware, devices, network equipment, or removable storage media to SSHIX-managed systems or networks.
- Install or use unauthorized software, applications, utilities, browser extensions, scripts, or other technology on SSHIX-managed systems.
- Introduce or intentionally facilitate the introduction of malware, viruses, ransomware, key-loggers, Trojans, spyware, or other malicious code.
- Use peer-to-peer file-sharing services or other unauthorized file-transfer technologies.
- Establish or use unauthorized remote-access connections, remote-control software, virtual private networks, tunneling technologies, or other mechanisms intended to bypass established access controls.
- Use technology or services in a manner that interferes with the normal operation, availability, performance, or security of SSHIX systems.

3.3 Protection and Handling of Sensitive Data

Users shall not:

- Access, use, copy, alter, disclose, transmit, retain, or destroy Sensitive Data except as necessary to perform an authorized business function.
- Access or use more information than is reasonably necessary to perform the user's authorized function.
- Copy, download, or store SSHIX Sensitive Data on personally owned devices, removable media, personal storage locations, or other unauthorized systems.
- Send or forward SSHIX Sensitive Data to personal email accounts.
- Upload, enter, transmit, disclose, or otherwise provide SSHIX Sensitive Data to unauthorized websites, cloud services, file-sharing platforms, artificial intelligence systems, collaboration tools, or other external services.
- Transmit PII, PHI, or other Sensitive Data using methods that have not been authorized for the type and sensitivity of information involved.
- Transmit Federal Tax Information, including IRS Forms 1095-A, through email, fax, or any other method prohibited by applicable IRS requirements or SSHIX policy.
- Photograph, record, capture, reproduce, or otherwise retain Sensitive Data using unauthorized devices or applications.

3.4 Electronic Communications

Electronic communication tools used for SSHIX business shall be used professionally and only through authorized methods.

Users shall not use email, messaging platforms, collaboration tools, text messaging, video conferencing, or other electronic communication tools to send, forward, post, upload, or otherwise transmit:

- PII, PHI, or other Sensitive Data without appropriate authorization and required safeguards.
- Federal Tax Information through a prohibited communication method.
- Content that is unlawful, discriminatory, harassing, defamatory, obscene, threatening, sexually explicit, or otherwise inconsistent with applicable State, NVHA, SSHIX, or employer policies.
- Chain letters, unauthorized solicitations, or materials related to personal commercial ventures.
- Copyrighted, licensed, or proprietary materials when the user is not authorized to reproduce, distribute, or transmit such materials.

Users shall not use unauthorized external messaging, collaboration, file-sharing, or communication services to conduct SSHIX business or to transmit or store SSHIX information.

3.5 Internet and External Service Use

Users shall not use SSHIX systems or network resources to access, download, upload, transmit, or distribute content or services that:

- Are unlawful or inconsistent with applicable State, NVHA, SSHIX, or employer policy.
- Contain sexually explicit, pornographic, harassing, discriminatory, threatening, or otherwise inappropriate material.
- Support unauthorized gambling, commercial activities, or personal financial gain.
- Contain malware, malicious code, or software that SSHIX is not authorized or licensed to use.
- Create an unreasonable security risk or interfere with SSHIX business operations.
- Result in unauthorized disclosure, storage, or processing of SSHIX Sensitive Data.

3.6 Personal Use

SSHIX systems and resources are intended primarily for authorized business purposes.

Where permitted by the user's employer and applicable SSHIX policy, limited incidental personal use may be permitted provided that such use:

- Does not interfere with the user's work responsibilities or SSHIX business operations.
- Does not consume unreasonable system, network, or personnel resources.
- Does not result in additional or inappropriate cost to SSHIX or the State.
- Does not involve outside business activities, commercial ventures, fundraising, political activity, or other unauthorized activities.
- Does not violate any applicable federal or State law, regulation, agreement, security requirement, or organizational policy.
- Does not result in the storage, transmission, or processing of SSHIX Sensitive Data through unauthorized systems or services.

3.7 Security and Privacy Violations

Users shall not knowingly conceal, alter, destroy, or withhold information relevant to security, privacy, compliance, or administrative investigation.

Users shall not interfere with or attempt to prevent authorized security monitoring, auditing, logging, vulnerability assessment, incident response, forensic examination, or other security activities conducted by or on behalf of SSHIX, NVHA, or the State of Nevada.

Users shall promptly report suspected or actual unauthorized access, credential compromise, malware, loss or theft of devices or information, improper disclosure of Sensitive Data, or other suspected security or privacy violations in accordance with SSHIX reporting procedures.

Complaints

Suspected violations of this agreement shall be reported through the appropriate SSHIX reporting channel. Privacy concerns or suspected improper handling of PII, PHI, or FTI shall be reported to the SSHIX Privacy Officer by emailing privacy@nvha.nv.gov. Suspected cybersecurity incidents, credential compromise, malware, unauthorized system access, or other security events shall be promptly reported to the SSHIX Information Security Officer or other designated security reporting channel.

Sensitive information, passwords, authentication credentials, FTI, or unnecessary PII/PHI shall not be included in an initial email notification.

Consequences

Violation of this Acceptable Use Agreement may result in restriction, suspension, or revocation of access to SSHIX systems or information and other corrective action appropriate to the individual's relationship with SSHIX.

For SSHIX or State employees, violations may result in disciplinary action in accordance with applicable personnel policies, up to and including termination of employment.

For contractors, insurance carrier personnel, business partners, agents, or other external users, violations may result in notification to the individual's employer or sponsoring organization, suspension or termination of access, removal from authorized functions, contractual remedies, or other action available to SSHIX or the State of Nevada.

Violations may also be referred to law enforcement, regulatory authorities, or other appropriate entities when required or authorized by law.

Definitions

Authentication Credentials:

Any information, device, token, certificate, biometric factor, password, passphrase, authentication application, MFA approval, or other mechanism used to verify identity or authorize access.

Authorized Use:

Use of SSHIX systems, networks, and data that is explicitly approved for official business purposes in accordance with job duties, policy, and management direction.

Personally Identifiable Information (PII):

Any information that can be used to identify an individual, either on its own or when combined with other data.



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

Examples include full name, date of birth, Social Security Number, mailing address, phone number, and government-issued ID numbers.

Protected Health Information (PHI):

Health-related information that is linked to an individual and is protected under HIPAA. This includes medical records, treatment details, insurance information, and any health data tied to a person's identity.

Security Incident:

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information it processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, procedures, or acceptable use requirements.

Sensitive Data

Includes PII, PHI, Federal Tax Information (FTI), financial information, authentication information, confidential business information, and any other information classified as confidential, restricted, or otherwise requiring protection under applicable federal, State of Nevada, NVHA, or SSHIX requirements.

SSHIX Systems and Information:

Information systems, applications, networks, technology resources, and data owned, operated, managed, or made available by or on behalf of SSHIX, including the Nevada Health Link platform and supporting services.

Electronic Communication Tools

Any technology used to send, receive, or store messages or data as part of SSHIX business operations. This includes, but is not limited to, email, phone calls, voicemail, text messages, instant messaging apps (e.g., Microsoft Teams, Slack), video conferencing platforms, and internal chat systems; regardless of whether accessed via agency-issued or personal devices.

Document Revision History

Version	Issue Date	Changes	Drafted	Approved
1.0	June 3, 2019	Initial Release	R. Cook	R. High
20.01	May 18, 2020	No changes; 2020 annual review	R. Cook	R. High
21.01	May 12, 2021	No changes; 2021 annual review	R. Cook	R. High
22.01	May 05, 2022	No changes; 2022 annual review	R. Cook	R. High
23.01	May 15, 2023	No changes; 2023 annual review	R. Cook	R. High
24.01	May 01, 2024	No changes; 2024 annual review	M. Borgman	R. Cook
25.01	June 13, 2025	No changes; 2025 annual review	M. Borgman	J. Davis
25.02	July 01, 2025	Added handling of PII, PHI, Definitions and updated Consequences.	M. Borgman	J. Davis
26.01	August 26, 2026	NVHA letterhead; consolidate overlapping provisions and better align the Acceptable Use Policy with current NVHA/SSHIX security expectations.	J. Davies, NVHA Information Security Officer	S. Moses, Chief Operations Officer



Jennifer Krupp, MPH, MBA, PHP, Administrator
Division of Consumer Health Services



Stacie Weeks, JD, MPH, Director
Nevada Health Authority

Silver State Health Insurance Exchange

Acknowledgment of Acceptable Use Agreement

I acknowledge that I have received, read, understand, and agree to comply with the SSHIX Acceptable Use Agreement and applicable privacy and information security requirements governing my access to SSHIX systems and information.

I understand that access to SSHIX systems and information is provided solely for authorized purposes and that my activities may be monitored, logged, reviewed, or audited as permitted by applicable law and policy.

I understand that violations of these requirements may result in restriction or revocation of access, disciplinary or contractual action, and other consequences as authorized by law, regulation, policy, or agreement.

NAME (please print)	
SIGNATURE	
EMPLOYER (LEGAL NAME)	
DATE	