NV-HIE Policy Introduction

Establishing information sharing policies are among the most fundamental and critical decisions to be made for any effort to exchange or share health information, whether being pursued inside or outside of government. Coming to an agreement on workable policies requires broad, object involvement in order to get appropriate and relevant feedback and secure early buy-in as well as ongoing support for the initiative from various constituents and the public at large. Public trust will occur through both sound policies and an inclusive process, which also includes having consumers at the decision-making table. Since NV-HIE's foundation is to have stakeholders input and involvement in all of its initiatives, the NV-HIE policies will be continuously reviewed and revised by various stakeholders throughout the state involved in NV-HIE and health care legal and policy initiatives.

The Office of the National Coordinator for Health Information Technology (ONC) information regarding *Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program*, the Office of Civil Rights (OCR) information regarding the HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment in conjunction with *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (the Privacy and Security Framework) and the Markle Foundation's *Connecting for Health Common Framework* were utilized as reference material in the development of these policies. These guidance illustrated how HIPAA covered entities may utilize the Privacy Rule's established baseline of privacy protections and individual rights with respect to individually identifiable health information to elicit greater consumer confidence, trust, and participation, in electronic health information exchange.

NV-HIE with stakeholder involvement will review and update the Policy Manual at least annually to comply with changes in the law, including relevant standards and implementation requirements of Federal and State law.

POLICY: Authorized Users Information and Types	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To outline the process used to designate the authorized users of NV-HIE information and types of information that can be accessed.

A. Authorized Users

1. Participants are responsible for designating the "Authorized Users" within their organizations who will use the Exchange, including but not limited to employees and medical staff members.
2. Each Participant must designate the Privacy and/or Security Administrator and provide that persons' contact information to NV-HIE.
3. The Security Administrator is responsible for identifying Authorized Users, assigning the appropriate security level for each Authorized User and obtaining organizational approval of proposed Authorized Users.
4. Each Participant and NV-HIE shall have an authorization process in place to ensure users have access to only those applications and the protected health information that they are allowed to use or review.
5. NV-HIE will accept requests for user IDs and passwords only from an organization's designated Security Administrator or personnel.
6. NV-HIE may designate staff or support personnel as "Authorized Users" who will use NV-HIE for maintenance, testing, training, and/or operations of NV-HIE.
    i. NV-HIE will be responsible for assigning the user IDs and passwords and assigning the appropriate security level for each NV-HIE Authorized User and obtaining organizational approval for proposed Authorized Users, i.e. Director of IT approval.

B. Required Information for Authorized Users

1. Access to the Exchange shall be based on the functional needs and job roles of each Authorized User.
2. Only the minimum access privileges necessary to perform a given job function should be requested by the Participant's Security Administrator, and only those will be granted by NV-HIE.
3. The information required for each user access request includes:
    i. First Name
    ii. Last Name
    iii. Title
    iv. Password
    v. Company Name

vi. Job Category
vii. Office Phone
viii. Office Fax
ix. Office address

4. The following are only applicable to provider user requests:
   i. Cell phone
   ii. Pager
   iii. NPI (National Provider Identifier)
   iv. Specialty
   v. DEA Number

C. **Authorized User Types**

1. Authorized Users are granted access to NV-HIE functions based on their job category.
2. Participants shall limit Authorized User access to the minimum necessary required by the Authorized User's job category.
3. A Participant may define Authorized User job categories and access rights in accordance with the Participant's specific organizational needs and structure.
4. NV-HIE reserves the right to review and approve the Participant-defined job categories and access rights.
5. To assist Participants in the developing Authorized User job categories and access rights, NV-HIE provides the following, non-exclusive recommendations:
   i. *MD, DO, DDS, DPM, Resident and Nurse Practitioner:* Write and sign prescriptions. Access, review and edit patient clinical data.
   ii. *Licensed Health Professional (PAs):* Write and sign prescriptions for supervising MD's review. Access and review patient clinical data.
   iii. *Staff 1:* Medical support of clinical staff members who need to draft prescriptions and/or access patient clinical data, after the patient record has been accessed in the clinical workgroup.
   iv. *Staff 2:* Registration staff who have access only to demographic and health insurance eligibility information.
   v. *Lab/Radiology Staff:* Lab and radiology technicians or support staff who will access patient demographics and clinical data for electronic ordering.
   vi. *HIM Staff:* HIM professional or support staff will have full viewing right to demographic information and patient clinical data.
   vii. *Designated Security Administrator:* Designated Security Administrator will have rights for identifying users, assigning the appropriate security level for each user and obtaining organizational approval of those users.
6. An Authorized User of NV-HIE will be assigned a unique User ID, password and/or other security measures associated with and based on the specific user's role and job category. The users ID and passwords may not be shared with others.
7. The Authorized User's right to access clinical data through NV-HIE will be terminated upon termination of the Authorized User's employment or relationship with the

Participant or upon any violation by the Authorized User of the Participation Agreement or the provisions of the Participant's Privacy and Security Policies or NV-HIE's Policy Manual.

8. An Authorized Users' viewing rights will be defined by the Participants and defined by their role with the Participant. These may include:
    i. Clinician with full viewing rights
    ii. Other personnel with full viewing rights (to include only such individuals with need and reason to access clinical data who are authorized to access clinical data under applicable laws and regulations)
    iii. Other personnel with limited viewing rights: these individuals will have access to only patient search and Participant's status screens in NV-HIE.

D. **Breaking the Glass:**

1. Only an Authorized User who is treating the patient may Break the Glass, i.e. access all of that patient's Confidential Health Information notwithstanding the absence of a Patient Choice Election Form or Patient Authorization Record permitting such access, if consent by or on behalf of the patient is not reasonably possible, and in the professional judgment of the Authorized User, access to such Confidential Health Information is necessary to ensure optimal Treatment of the patient. Notwithstanding the foregoing, an Authorized User may not access such information if the Patient Choice Election Form or Patient Authorization Record indicates that the patient elected not to participate in NV-HIE.
2. Each time an Authorized User seeks access to a patient's Confidential Health Information under the circumstances detailed in the preceding paragraph, the Authorized User will be asked to certify that obtaining consent by or on behalf of the patient is not reasonably possible, and that, in the professional judgment of the Authorized User, access to such Confidential Health Information is necessary to ensure optimal Treatment of the patient. Authorized Users will not be permitted to access any Confidential Health Information without providing this certification.
3. Any access by an Authorized User to Confidential Health Information will be subject to an audit trail function that allows tracking and auditing of such access.

E. **Sensitive patient health information**, (e.g. HIV/AIDS, sexually transmitted diseases, substance abuse, mental health conditions), is restricted from access for most purposes. This information can only be accessed with patient's consent and under an "opening the privacy seal" access process and only by a clinician.

F. **Termination of Access:**

1. An Authorized Users' access shall cease upon termination of that Authorized User by Participant.
2. Any Authorized Users failing to act in accordance with the Participation Agreement or NV-HIE's policy manual will be disciplined.
    i. Participant's Authorized Users may have their access temporarily disabled;
    ii. Participant will be notified immediately of the concern or unauthorized access;

iii. NV-HIE will coordinate solution with Participant to mutual agreement.

3. Designated NV-HIE staff's access will be terminated upon termination of employment. In addition, staff's access will be temporarily disabled in accordance with NV-HIE policies and the employee will be disciplined in accordance with NV-HIE policies and procedures. Such disciplinary action may include termination.

For access descriptions, processes for "opening the privacy seal", and list of reasons for "breaking the glass", see *Users Permission Policy.*

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Accountability Principle in the Privacy and Security Framework	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To ensure a process is implemented, and adherences assured, through appropriate monitoring and other means and methods to report and mitigate non-adherence and breaches.

PROCESS

1. Participating organizations as the covered entities that exchange protected health information (PHI) to and through NV-HIE will comply with the HIPAA Privacy Rule administrative requirements and extend such obligations to NV-HIE as a business associate.
2. Participating organizations as the covered entities are responsible for their own non-compliance with the HIPAA Privacy Rule, as well as that of their workforce.
3. NV-HIE, through its business associate agreement with the participating organization, will be contractually obligated to adequately safeguard the PHI and to report noncompliance with the agreement terms to the participating organization/covered entity, and the covered entity will be held accountable for taking appropriate action to cure known noncompliance by NV-HIE, the business associate, and if unable to do so, to terminate the business associate relationship.
4. NV-HIE may provide satisfactory assurances as part of its business associate agreement that adequately safeguard PHI. These may include:
    a. NV-HIE will not use or disclose PHI except as allowed by the agreement
    b. NV-HIE will implement reasonable and appropriate safeguards for PHI
    c. NV-HIE will report any uses or disclosures of PHI that violate the agreement of the participant/covered entity.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: : Access to NV-HIE in accordance with HIPAA Privacy Rule	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To outline the protocol used to determine who has authorized access to NV-HIE, both in data sharing and accessing the information.

PROCESS

1. Access to NV-HIE will only be provided to Participant organizations which have a signed Participation Agreement and Business Associate Agreement with NV-HIE and are authorized to access data in accordance with HIPAA Privacy Rule.
2. Data shared with NV-HIE on behalf of Participants/Providers/Payers will only be used for treatment and/or business operations as outlined in the HIPAA Privacy Rule. This may include submitting Participant/Provider/Payer information for public health reporting or to health oversight agencies at the state and federal level, i.e. immunizations, syndromic surveillance, registries, etc.
3. As defined by the HIPAA Privacy Rule, Participants as covered entities may use NV-HIE to facilitate the exchange of PHI to other health care providers for treatment purposes, after initiation of the business associate agreement.
4. NV-HIE may also receive PHI and manage, as a business associate on behalf of Participants, a master patient index for purposes of identifying and linking all information about a particular individual. Disclosures to, and use of, NV-HIE for such purpose is permitted as part of the Participant's health care operations.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Compliance with Privacy and Security Laws and Protocol	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To outline the protocol used to maintain the confidentiality, privacy and security of individuals' protected health information in accordance with applicable state and federal regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

PROCESS

1. **Compliance with Privacy Laws, Regulations and Policies:**

    a. All Participants must comply with state and federal laws and regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), related to the use and disclosure of Confidential Health Information.

    b. NV-HIE has implemented appropriate operational and technical safeguards to prevent the improper use and disclosure of Confidential Health Information. In the same way Participants must safeguard Confidential Health Information contained in records within their facility, they have the responsibility not to use or disclose information obtained through NV-HIE inappropriately.

2. **Responsible Parties:**

    a. NV-HIE's Director of IT is the designated NV-HIE Privacy and Security Officer.

    b. NV-HIE's Director of IT or designee of NV-HIE has primary responsibility for execution and revision of the privacy and security policies, for ensuring audits occur by NV-HIE staff and that results and corrective actions are undertaken and reported as appropriate. The Director of IT or his/her designee will oversee the activities of NV-HIE to evaluate compliance by Participants with this policy and enforce its terms.

    c. An annual privacy and security internal audit plan will be developed by the Director of IT or designee based on guidance from ONC and HIPAA regulations. This plan will receive input and direction from NV-HIE's Technical Committee and NV-HIE's Board of Directors will be the governing body for final approval.

    d. Annually, the results of the privacy and security audits will be presented to NV-HIE's Board of Directors for final approval.

e. Participants will have the responsibility to ensure compliance with state and federal laws and regulations, such as HIPAA, to maintain the confidentiality, privacy and security of individuals' protected health information.

3. Business Associate Agreements:

a. NV-HIE will enter into a Participation Agreement with each Participant, which agreement shall include a Business Associate Agreement as required by 45 C.F.R § 164.502(e). NV-HIE will ensure that all its contracts and contracts of any subcontracts include a Participation Agreement and/or Business Associate Agreement to the extent required by 45 C.F.R § 164.502(e).

4. Security Practices:

a. Tracking. Any access by an Authorized User to Confidential Health Information through NV-HIE will be subject to an audit trail function that allows tracking and auditing of such access.

b. Confidentiality and Re-disclosure. Each Participant shall keep confidential any Confidential Health Information obtained through NV-HIE and shall only re-disclose such Confidential Health Information as authorized by law.

c. Virus Protection Software. Each Participant shall install, maintain and update virus protection software that meets minimum standards established by NV-HIE as well as HIPAA regulations on all of its computers used for the purpose of accessing Confidential Health Information through NV-HIE.

d. Notification to NV-HIE. Each Participant shall promptly notify NV-HIE of any use or disclosure of Confidential Health Information in violation of this policy or any related security breach of which it becomes aware. Notwithstanding the foregoing, notification shall be made within 24 hours of actual knowledge. Each Participant shall, in consultation with NV-HIE, take reasonable steps to mitigate the potentially harmful effects of any such incident.

e. Additional Privacy and Security Measures. Participants shall adopt and implement any other privacy and security policies and procedures relating to the use, maintenance and disclosure of Confidential Health Information obtained through NV-HIE that are necessary to assure the Participant's compliance with HIPAA and all other applicable confidentiality laws and regulations. Additionally, NV-HIE and Participants will implement "reasonable and appropriate" safeguards to protect the security of PHI.

5. Participants Responsibility for Authorized User Compliance

a. Limits on Use. Confidential Health Information obtained by an Authorized User through NV-HIE may be used or disclosed by the Authorized User for treatment or health care operations purposes only.

b. HIPAA Training for Authorized Users. Each Participant is responsible for training of all its Authorized Users on compliance with this policy, the HIPAA regulations, other applicable privacy laws and rules and the Participant's privacy and security policies. Each Participant will require each Authorized User to execute an Authorized User Agreement. Authorized Users will include only those individuals who require access to NV-HIE to facilitate use of the Data for a Permitted Use. Participant is responsible for its Authorized Users compliance with the terms and conditions of the Participation Agreement and applicable laws and regulations.

c. Discipline for Violations. Each Participant shall be responsible for disciplining any of its Authorized Users who violate the terms of this policy, HIPAA or other applicable laws and regulations in accordance with its own policies and procedures. Notwithstanding the foregoing, NV-HIE reserves the right, in its sole discretion, to terminate (or cause the applicable Participant to terminate) the access to NV-HIE of any Authorized User who violates the terms of this policy, HIPAA or other applicable laws or regulations.

d. Audits. NV-HIE will conduct periodic audits of appropriate access to Confidential Health Information in accordance with NV-HIE's audit policies. Participants are also encouraged to conduct periodic audits of appropriate access to their patient's Confidential Health Information in accordance with their privacy and security policies.

6. Access by NV-HIE and NV-HIE staff

a. Notwithstanding anything to the contrary set forth in these Policies, NV-HIE and NV-HIE staff shall not have access to any Confidential Health Information through the NV-HIE System other than in connection with the performance of audits in accordance with the Audit Policy, testing the functionality and operational support of NV-HIE; provided that NV-HIE/NV-HIE staff's access to Confidential Health Information shall be limited only to such information as may be reasonably necessary for such auditing, testing and/or operational support functions.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Confidentiality and Security of Protected Health Information	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To outline the standards used to maintain the confidentiality, privacy and security of individuals' protected health information in accordance with applicable state and federal regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

RESPONSIBILITY

All NV-HIE employees involved in the access, use, release or disclosure of an individual's protected health information (PHI). If a business partner has a different policy or contractual requirements, employees are expected to also comply with the business partner's policy or contractual requirements. This policy applies to NV-HIE in its role as the business associate of HIPAA defined covered entities.

PROCESS

A. Minimum Requirements

1. Reasonable efforts must be made to use, disclose or request only the minimum amount of PHI to accomplish the intended business objective.

2. Generally, only the narrowest or least amount of PHI is used or disclosed, covering the shortest period of time, to address the business objective for which the information is needed, and no more.

3. In addition, the use of PHI should be by, or disclosure should be to, only that person or those persons with a need-to-know, and who require the PHI to perform their functions or to accomplish a specific business objective.

4. When using or disclosing PHI for the following purposes, there is no minimum necessary requirement:

   a. Treatment – disclosures to or requests by a healthcare provider for treatment to an individual;
   b. Individual – permitted or required disclosures to, or requests by, an individual of his/her own information;
   c. Authorized uses or disclosures – uses or disclosures authorized by an individual;
   d. U.S. Department of Health and Human Services (HHS) – disclosures to HHS for investigation of HIPAA complaints;
   e. Required by law – disclosures required by state or federal law; and
   f. Compliance – uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules.

B. Uses and Disclosures of PHI

1. Uses and disclosures permitted with the individual's authorization:

   a. An individual's PHI may be used or disclosed with the individual's (or individual's authorized personal representative's) authorization for any purpose. Such authorization from the individual must be documented.

2. Uses and disclosures permitted for payment or healthcare operations purposes that do not require the individual's authorization:

   a. An individual's PHI may be used or disclosed without the individual's authorization for purposes of conducting the payment activities or healthcare operations of the covered entity when NV-HIE is its business associate, or when the PHI is disclosed to NV-HIE' business associate. The minimum necessary standard applies to these uses and disclosures.

   b. The minimum necessary PHI may be disclosed to another covered entity (or at the direction of the covered entity) for the healthcare operations of the other covered entity if the PHI to be disclosed: (i) pertains to the relationship that both NV-HIE (or the covered entity) have or had with the individual who is the subject of the PHI; and (ii) the healthcare operations for which the disclosure is being made involves one of the following:

      1. Quality assurance
      2. Competency assurance
      3. Fraud and abuse control

3. Uses and disclosures that require authorization from an individual:

   a. Except for purposes of treatment, payment activities or healthcare operations, or as otherwise permitted or required by state or federal law, an individual's authorization must be requested prior to the use or disclosure of the individual's PHI.

   b. An authorization is required to use or disclose PHI for marketing purposes that do not involve:

      i. Communications about health-related products or services provided by, or included in a plan of benefits, or other value-added health-related products or services offered by the company;
      ii. Distributing promotional items of nominal value; and
      iii. Face-to-face communications by the company to the individual.

   c. Activities requiring an authorization include those involving the use or disclosure of PHI maintained by NV-HIE, such as brand name marketing, direct mail or telemarketing for non-health-related products or services (e.g., life insurance, disability, etc.) or newsletters with articles about non-health-related products or services.

d. An individual's authorization is required prior to the use or disclosure of an individual's psychotherapy notes (defined by HIPAA as notes recorded by a healthcare provider who is a mental health professional documenting or analyzing the contents of a conversation during a private, group or family counseling session and that are separated from the rest of the individual's' medical record).

4. De-identified health information

a. There are no minimum necessary or authorization restrictions on the request for, or use or disclosure of, de-identified health information. PHI can be de-identified in one of two ways:

i. Remove identifiers: if all of the following identifiers of the individual, his/her relatives, his/her employers or his/her household members are removed, and the employee using or disclosing the information has no actual knowledge that the information could be used alone or in combination with other information to identify an individual:
- Names;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission and discharge date, date of death, all ages over 89;
- Telephone or fax numbers, e-mail addresses;
- Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers;
- Certificate-license numbers, vehicle identifiers, device identifiers;
- Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers;
- Biometric identifiers, full face photographic images and any comparable images;
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code; and
- Any other unique identifying number, characteristic, or code (except re-identification codes).

ii. Statistical method: It is determined that the risk is very small that the PHI could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the PHI, based on generally accepted statistical and scientific principles and methods.

5. Disclosures permitted for purposes other than treatment, payment or healthcare operations

These disclosures do not require an authorization or other permission from the individual, but must meet the minimum necessary requirement and must be reported to NV-HIE's Executive Director (or the customer's/covered entity's Privacy Officer) to be tracked for purposes of providing an accounting of disclosures:

a. Health and safety purposes – disclosures to the extent necessary to avert a serious and imminent threat to an individual's health or safety of others, to a government agency authorized to oversee the healthcare system or government programs or its contractors, or to public health authorities.

b. Public health activities – as permitted or required by law. For example, disclosures for the purposes of preventing or controlling disease, injury or disability; investigation of reportable diseases; the control of public health hazards; enforcement of sanitary laws; certification and licensure of health professionals and facilities; and review of healthcare that is required by the federal government and other governmental agencies.

c. Health oversight activities – disclosure of PHI to a health oversight agency for activities authorized by law, such as audits, investigations, inspections, licensure or disciplinary actions, or civil, administrative, or criminal proceedings or actions.

d. Required by law – PHI may be disclosed if required by law. There is no minimum necessary requirement for these disclosures.

e. Legal, judicial and administrative proceedings – the minimum necessary PHI may be disclosed in response to a court or administrative order, subpoena, discovery request or other lawful process, in accordance with specified procedural safeguards. Subpoenas received for purposes other than health information management (HIM) routine operations should be referred to the NV-HIE Legal Counsel.

C. Business Associates

1. A business associate is a person or entity, other than a NV-HIE employee, that performs or assists in performing, a function or activity that involves the use or disclosure of PHI on behalf of NV-HIE.

2. NV-HIE contracts with business associates and also functions as the business associate of other covered entities.

3. Prior to the disclosure of PHI to a business associate, or prior to the business associate being allowed to create or receive PHI, "satisfactory assurances" will be obtained in the form of a written agreement that the business associate will appropriately safeguard and limit their use and disclosure of the PHI.

4. The NV-HIE Legal Counsel must review all business contracts to determine whether business associate requirements should be added to the contract.

D. Individual Rights

Requests for the following individual rights will be coordinated by NV-HIE's Chief Executive Officer or at the direction of the covered entity's Privacy Officer:

1. Access – Individuals have the right to inspect and obtain a copy of the PHI contained in their designated record set for as long as the information is maintained. Designated record set is defined as a group of records maintained by NV-HIE or its business associates, which is used to make treatment decisions about individuals.

2. Amendment – Individuals have the right to request amendment of their PHI and other records contained in their designated record set for as long as the designated record set is maintained. *See Correction Policy*

3. Accounting of disclosure – Individuals have the right to an accounting of the disclosures of PHI that were made after April 14, 2003, for purposes other than treatment, payment or healthcare operations, or other than pursuant to a valid authorization when such authorization is required. It is the responsibility of the Compliance Department (or covered entity's Privacy Office) to ensure that each disclosure made that is not exempted from the accounting requirement is documented. *See Correction Policy*

4. Restriction on use or disclosure – Individuals have the right to request that the use or disclosure of their PHI be restricted, including uses and disclosures made for treatment, payment or healthcare operations. NV-HIE does not have an obligation to agree to the request, but if agreed to, NV-HIE will comply with the agreement and notify any business associates of such agreement. *See Correction Policy*

5. Confidential communications – Individuals have the right to request that NV-HIE use alternative means or alternative locations (street address and/or telephone number) when communicating PHI to them.

F. Complaint Management

1. Any workforce member who suspects that the privacy or security policies and procedures, the HIPAA privacy or security rules, or other applicable federal or state privacy laws have been violated must report the suspicion to the Chief Executive Officer in sufficient detail to permit the matter to be investigated and to prevent or mitigate any deleterious effects.

2. All privacy and security complaints will be fully investigated, and appropriate actions taken, including, but not limited to:

    i. Technical system modifications;
    ii. Modifying or expanding audits;
    iii. Re-educating staff; and/or
    iv. Strengthening departmental procedures.

3. Employees that violate the privacy or security policies, the HIPAA privacy or security rules, or other applicable federal or state laws will be subject to disciplinary action as outlined in the NV-HIE Employee Manual. The NV-HIE Chief Executive Officer will act promptly to mitigate, to the extent possible, any harmful effect of improper use or disclosure of PHI.

G. Employee Training and Management

1. Orientation and training

   a. All new hires are given information on NV-HIE's Code of Corporate Conduct and NV-HIE's Employee Manual.

   b. New hires must complete the NV-HIE training program, which contains training on HIPAA privacy and security, within 60 days of hire.

2. Access to information

   a. Workforce members authorized to have access to PHI (and electronic PHI) to perform their job functions shall have access only to that level of information necessary to complete their job functions.

3. Documentation and retention

   NV-HIE will maintain in written or electronic form for six years from the date of creation or last effective date, whichever is later:

   a. NV-HIE's privacy and security policies and each revision of them;
   b. Each request from individuals for access, amendment, disclosure accounting, restriction or confidential communications and all documentation relating to them;
   c. Each complaint related to a real or perceived privacy or security violation and supporting documentation; and
   f. Other documentation requested or required by state or federal law, or this policy.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Correction Policy	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To provide individuals with a timely means for patient corrections within the Nevada Health Information Exchange, including the ability to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.

PROCESS

1. Individuals have the right to have their protected health information (PHI) amended in a manner that is fully consistent with the Correction Principle in the Privacy and Security Framework. (See 45 C.F.R § 164.526.)
2. The HIPAA Privacy Rule designated the Participant/covered entity as the responsible party for acting on an amendment or correction request from an individual/patient.
3. NV-HIE, acting as a business associate of the covered entity, can assist the covered entity in informing other Participants in NV-HIE who are known to have the individual's information, of the amendment by efficiently disseminating amended information to appropriate recipients throughout the electronic exchange.
4. Participants must take action in a timely manner, usually within 60 days, to correct the record as requested, with an additional 30 day extension in certain circumstances, or to notify the person if the request is denied.
5. A request may be denied if the Participant determines that the information is complete and accurate, and on limited other grounds.
6. When a request is denied, but the individual continues to dispute the accuracy of the information, the individual must be provided an opportunity to file a statement of disagreement with the covered entity and the covered entity must provide documentation of the dispute with any subsequent disclosure of the disputed PHI.
7. Through NV-HIE, the covered entity should be able to identify other Participants that maintain information on the individual and who, therefore, should be notified of the amended information.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

Nevada Health Information Exchange

POLICY: Corrective Action Policy	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To outline the process to be taken as corrective action upon identification and/or notification of noncompliance, either by a Participant or staff of NV-HIE.

PROCESS

1. According to NV-HIE policy ("NV-HIE Audit Policy"), if an audit reveals noncompliance, a corrective action plan must be submitted by the Participant to the NV-HIE's Director of IT or designee.

    a. The Director of IT or designee will forward the matter to the NV-HIE Chief Executive Officer.
    b. The Director of IT or his/her designee will make a recommendation on the corrective action plan to NV-HIE Chief Executive Officer as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Chief Executive Officer or be rejected.
    c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Chief Executive Officer after obtaining advise of Legal Counsel may decide to suspend access to the Exchange for either the Participant or one or more Authorized Users of such Participant until the problem is adequately addressed.

2. If an audit reveals noncompliance by a NV-HIE staff, a corrective action plan must be submitted to the NV-HIE's Director of IT or designee.
    a. The Director of IT or designee will forward the matter to the NV-HIE Chief Executive Officer.
    b. The Director of IT or his/her designee will make a recommendation on the corrective action plan to NV-HIE Chief Executive Officer as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Chief Executive Officer be rejected.
    c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Chief Executive Officer after obtaining advice of Legal Counsel may choose to take necessary disciplinary action against the employee and suspend access to the Exchange for the employee until the problem is adequately addressed.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Data Breach Notification and Investigation	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To facilitate compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) breach notification and investigation of unsecured protected health information (PHI) requirements.

DEFINITIONS

The following definitions apply to all of NV-HIE's privacy and security policies and procedures:

1. **Breach** – Unauthorized acquisition, access, use, or disclosure of unsecured, unencrypted protected health information which compromises the security or privacy of such information and poses a significant risk of financial, reputational, or other harm to the individual. To determine if a notification is required, a risk assessment must be performed to determine if the security or privacy of the PHI has been compromised (see Appendix A). The term 'breach' does not include:
    a. Any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate if
        i. Such acquisition, access, or use was made in good faith and within the course and scope of authority;
        ii. Such information is not further used or disclosed in a manner not permitted; or
        iii. Any inadvertent disclosure by a person who is authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates; and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
        iv. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. **Protected Health Information** – Any oral, written or electronic individually-identifiable health information collected or stored by a covered entity or business associate. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.

3. **Unsecured PHI** - Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology

specified by the U. S. Secretary of the Department of Health and Human Services (HHS). At this time, the only technology is encryption; the only methodology is destruction.

PROCESS

1. Any Participant and/or NV-HIE employee and/or support personnel in the case of a breach of unsecured PHI must notify NV-HIE Chief Executive Officer or designee upon suspicion or knowledge of a breach within 24 hours.

2. If notification is received from a NV-HIE employee or support personnel and the breach involves a customer's PHI, the Chief Executive Officer shall coordinate with the appropriate NV-HIE Client Executive to provide notification to the customer's Compliance and/or Privacy/Security Officer without unreasonable delay.

3. A breach is considered discovered as of the first day on which the breach is known by the Participant and/or NV-HIE employee or support personnel.

4. If a law enforcement official determines that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed in the same manner as provided under §164.528(a)(2) of title 45, Code of Federal Regulations.

5. If a data breach occurs involving a customer's PHI, NV-HIE's Chief Executive Officer or her designee will provide the same information as in the Content of Notification (below) to the customer's Compliance and/or Privacy Officer without unreasonable delay for completion of the risk assessment and determination of notification.

6. Participants and NV-HIE are responsible for immediately investigating and mitigating to the extent possible, any privacy and/or security breach that they become aware of. They shall immediately:
    a. Investigate the scope and magnitude of the breach.
    b. Identify the root cause of the breach.
    c. Mitigate the breach to the extent possible.
    d. Notify all appropriate parties, i.e. NV-HIE Chief Executive Officer, Participant's Privacy and Security Officers, etc., within 24 hours of actual knowledge and the potential impact of the breach.
    e. In the event that the breach involves or may involve more than one Participant, Participants shall cooperate with NV-HIE and other Participant(s) in investigating and mitigating the breach, including but not limited to sharing any information that may be necessary in connection with such investigation and/or mitigation, subject to all applicable laws and regulations.

f. Notify regulatory agencies and customers in compliance with all applicable state and federal laws, rules and regulations.
g. Notify individuals affected by the breach as required by HIPAA.

7. NV-HIE Director of IT will provide a report of the breach and mitigation actions to the NV-HIE Chief Executive Officer, its Legal Counsel, and NV-HIE Board of Directors.

8. NV-HIE shall maintain a log of any breaches meeting the HITECH definition that occur during a calendar year. This documentation must be retained for a period of six years.

Content of Notification

The notice of the breach must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

2. A description of the type of unsecured PHI that were involved in the breach, such as full name, Social Security Number, date of birth, home address, account number, diagnosis code or disability code. Only the generic type of PHI should be listed in the notice (i.e., date of birth rather than the patient's actual birth date).

3. The steps the individual should take to protect themselves from potential harm resulting from the breach.

4. A brief description of what NV-HIE is doing to investigate the breach, mitigate harm to the individual, and to protect against further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, website, or postal address.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

GENERAL BREACH PROCESS INFORMATION FOR COVERED ENTITIES

Breach Notification Process

Patient Notification

1. After a complete investigation, no later than 60 days from breach discovery, the covered entity must provide written notice to the patient or:
    a. If the patient is deceased, the next of kin or personal representative.
    b. If the patient is incapacitated/incompetent, the personal representative.
    c. If the patient is a minor, the parent or guardian.

2. Written notification must be in plain language at an appropriate reading level with clear syntax and language with no extraneous materials. Americans with Disabilities Act (ADA) and Limited English Proficiency (LEP) requirements must be met.

3. Written notification must be sent to the last known address of the patient or next of kin, or if specified by the patient, by encrypted electronic mail. The template letter in the HITECH Breach Notification Reporting Process must be used when sending written notification to a patient, personal representative, or next of kin.

4. In the case where there is insufficient or out-of-date contact information:
    a. For less than ten (10) individuals that precludes direct written notification to the patient, a substitute form of notice shall be provided such as telephone call.
    b. In the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information and contact information is not obtained, the covered entity must:
        i. Post a conspicuous notice for 90 days on the homepage of their website that includes a toll-free number; or
        ii. Provide notice in major print or broadcast media in the geographic area where the patient can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number must be included in the notice.

5. If the covered entity's Compliance Officer, in concert with the Legal Department/Team, determines a patient should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, the covered entity may, in addition to providing notice as outlined in steps 2-4 above, contact the patient by telephone or other means, as appropriate.

Media Notification

1. In the case where a single breach event affected 500 or more residents of the same State or jurisdiction, notice shall be provided to prominent media outlets. A jurisdiction is defined as a

geographic area smaller than a state (e.g., city, county). For example, if a single breach event affects 200 patients in California and 400 patients in Nevada, a notice to the media is not required because there were not more than 500 patients in the same State or jurisdiction affected. However, if a single breach event affects 500 patients in California and 500 patients in Nevada, a media notice is required in both Texas and Louisiana.

2. The covered entity's Compliance Officer shall work with the Legal Department/Team and the NV-HIE Chief Executive Officer to coordinate the notification.

HHS Notification

1. Notice must be provided by the covered entity without reasonable delay and in no case later than 60 days from the breach discovery to the U. S. Secretary of the Department of Health and Human Services (HHS) if a single breach event was with respect to 500 or more individuals regardless of the State or jurisdiction. The covered entity must use the electronic form available on the HHS website when notifying HHS of breaches involving 500 or more individuals.

2. If a breach is with respect to less than 500 individuals, the covered entity must use the electronic form available on the HHS website and submit to HHS no later than 60 days after the end of the calendar year in which the breach occurred.

3. The covered entity must maintain a log of any breaches meeting the HITECH definition that occur during a calendar year. This documentation must be retained for a period of six years.

Nevada Health Information Exchange

APPENDIX A

Assessment of the Risk of Harm to the Individual from a Violation of the Privacy Rule under HIPAA and the HITECH Act

Violations of the HIPAA Privacy Rule are evaluated for the potential for significant risk of financial, reputational, or other harm to the individual whose information was compromised. This risk assessment is completed and documented for every violation of the Privacy Rule involving unauthorized acquisition, access, use or disclosure of unsecured PHI that does not fit within an exception defined in the HITECH Act. When a violation is determined to result in significant risk of harm to the individual, notification to the individual and to the Secretary of HHS is required.

The following general framework is used to assess for risk depending upon the specific facts associated with the risk in order to determine whether breach notification is required.

1. Who are the parties involved in the incident?

   a. Is the individual who impermissibly used/disclosed the information an NV-HIE employee?

Lo	(1)	NV-HIE employee otherwise authorized to access the PHI
Lo	(1)	NV-HIE employee not otherwise authorized to access the PHI
Med	(2)	Non NV-HIE employee accessed/used/disclosed the PHI

   b. Who received the disclosed PHI?

Lo	(1)	Another NV-HIE employee not defined in the exceptions to breach
Lo	(1)	An individual that is a covered entity or a business associate
Med	(2)	An individual that is not bound by HIPAA and external to NV-HIE

2. What type(s) of information was disclosed?

   a. Limited Data Set

N/A	(0)	Not a Limited Data Set
Lo	(1)	16 HIPAA defined identifiers removed and also either no date of birth (DOB) or no zip code
Lo	(1)	16 HIPAA defined identifiers removed and age or zip codes do not create identifiable populations
Med	(2)	16 HIPAA defined identifiers removed, but ages or zip codes make re-identification possible

b. Direct Patient Identifiers

	N/A	(0)	No direct identifiers were disclosed
	Lo	(1)	Full name or partial name, but no contact demographic information (such as address or phone), may include medical record number but no Social Security number (SSN) or DOB
	Med	(2)	Name with phone number or address but no SSN or DOB
	Med	(2)	Full name with DOB
Mandatory	Hi	(3)	SSN (or credit card or bank account number) with first initial or first name and last name

c. Type of services provided

	N/A	(0)	No information regarding health services or care disclosed
	Lo	(1)	Identified as patient of an NV-HIE customer or customer's provider
	Med	(2)	Reason for receiving care; diagnosis or treatment; or test results disclosed
		(3)	"Sensitive" treatment revealed by location or a condition that might result in employment discrimination or reputational harm (e.g. HIV, Cancer, Substance Abuse, genetic disorders)

3. <u>What is the likelihood of unauthorized use or disclosure of the PHI?</u>

a. Lost or Stolen Device with ePHI

N/A	(0)	Not applicable
Lo	(1)	Device retrieved before it was accessed or device encrypted
Med	(2)	Device is known to be password protected but not encrypted
Hi	(3)	Device not known to be encrypted

b. Paper Media Breached (e.g. lost, stolen, faxed, or mailed)

N/A	(0)	Not applicable
Lo	(1)	Information is returned without seal on envelope being broken
Med	(2)	PHI is disclosed to someone who does not know the patient and who provides assurance the information has been returned and/or destroyed
Hi	(3)	PHI is disclosed to someone who may know of the patient and who is reasonably believed to have accessed the information

Nevada Health Information Exchange

Risk Assessment Scoring Grid

Question	Score	Notes
1 a.		
1 b.		
2 a.		
2 b.		
2 c.		
3 a.		
3 b.		
TOTAL		
KEY:	0-7	Low Risk of Harm to the Individual (notification not required)
	8 – 9	Medium Risk of Harm to the Individual (notification may be required; determined by business leader and Privacy Office based upon facts of specific event)
	10 or more	High Risk of Significant Harm (notification will generally be required unless an exception is determined based upon specific facts of the event)
	2. b. HI	Automatically triggers notification requirements under Federal law (and possible State law)
	2. c. HI	Automatically triggers notification if any 2.b. direct identifiers are also disclosed

Completed by:

Date:

POLICY: HIE External Evaluation	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

NV-HIE will evaluate the Nevada Health Information Exchange (NV-HIE) both internally and externally. These evaluations will provide information on the progress NV-HIE is making toward promoting the Nevada Health Information Exchange, the management of grant funds, the appropriate levels of stakeholder participation, and the overall impact that NV-HIE is having on the health of Nevada's citizens. The evaluation will also provide information to the federal government about the relative success of different approaches to implementing HIE, and the success of the grant funds in preserving and creating jobs.

PROCESS

1. NV-HIE's Vendor Selection Policy process will be followed in the securing of an external evaluator for the HIE.
2. NV-HIE will follow the ONC guidelines for obtaining an external evaluation process and ensure that adequate funds are utilized in accordance with their directive.
3. The HIE External Evaluation will be conducted on at least an annual basis.

The NV-HIE evaluation plan will be a two-tier approach with a number of quantitative metrics that can rather easily be obtained and a set of qualitative and quantitative assessments designed to delve deeper into the impact and success of NV-HIE and the grant. In general, evaluation efforts should include a focus on:

- Adoption/utilization
- Effectiveness
- Barriers/vulnerabilities

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Individual Access to PHI	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To ensure a process is implemented that allows individuals the right to access their protected health information (PHI), right to amend their PHIE, and accounting of disclosures of PHI.

PROCESS

1. Participating organizations as the covered entities that exchange protected health information (PHI) to and through NV-HIE will comply with the HIPAA Privacy Rule administrative requirements and extend such obligations to NV-HIE/NV-HIE as a business associate.
2. Participants as covered entities under the HIPAA Privacy Rule will have the opportunity to enable patients to have the right to make requests for access to their PHI, provided they inform individuals of such a requirement. (See 45 C.F.R. § 164.524(b)(2)(i).)
3. Participants shall develop and implement reasonable policies and procedures that outline the specific provisions of access, form or format of access provided, and denial of access process.
4. NV-HIE/NV-HIE may be permitted by the Participant/covered entity, acting as its business associate, to assign the appropriate credentials and authenticate personal representatives, and any others, seeking access to PHI.
5. Participants shall educate patients with respect to the terms and conditions upon which their health information is shared and their rights to access their own health information.
6. Patient access to health information must be in accordance with all applicable laws and regulations, included but not limited to, La. R.S. 40:1299.96(A)(2)(d) which allows a health care provider to deny access to a record if the health care provider reasonably concludes that knowledge of the information contained in the record would be injurious to the health or welfare of the patient or could reasonably be expected to endanger the life and safety of any other person, La. R.S. 40:1300.14 regarding confidentiality of HIV patients, and any and all state and federal laws permitting denial of access to medical information in specific circumstances.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Individual Choice for Sharing Information in NV-HIE	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

To provide guidelines defining the process of how individuals should be provided a reasonable opportunity and capability to make informed decisions about the use and disclosure of their individually identifiable health information as it relates to the Nevada Health Information Exchange (NV-HIE) and in alignment with the HIPAA Privacy Rule as it relates to the Individual Choice Principle in the Privacy and Security Framework.

PROCESS

1. As a HIPAA covered entity, each Participant that intends to electronically exchange protected health information (PHI) to and through NV-HIE, primarily for the purpose of treatment, will focus on how the Privacy Rule's provisions for optional consent and the right to request restrictions on certain uses and disclosures can support and facilitate individual choice with respect to the electronic exchange of health information in a networked environment.
2. Commencing the effective date of the Participation Agreement, each Participant that is providing data may elect to adopt an individual consent policy and, as part of the patient admission/registration process, offer each individual/patient the opportunity to make *meaningful choices* with respect to the electronic exchange of their individually identifiable health information.
3. A patient's *meaningful choice* means that choice is:
    a. Made with advance knowledge/time;
    b. Note used for discriminatory purposes or as condition for receiving medical treatment;
    c. Made with full transparency and education;
    d. Commensurate with circumstances for why PHI is exchanged;
    e. Consistent with patient expectations; and
    f. Revocable at any time.
4. Once an individual/patient has indicated his/her choice to participate in NV-HIE or not, the Participant is responsible for creating a record of the individual/patient's choice.
5. The Participant is responsible for noting in the NV-HIE system the individual/patient's choice and assuring that the presence of an appropriate Patient Authorization Record is maintained.
6. If obtained, each Participant must maintain documentation of each individual/patient's decision to participate or not participate in NV-HIE.
7. If the Patient Authorization Record indicates that the individual/patient has chosen to participate in NV-HIE, the individual/patient's Confidential Health Information will be exchanged.
8. The Privacy Rule also provides individuals/patients with a right to request that a covered entity restrict uses or disclosures of PHI about the individual for treatment, payment, or health care operations purposes. Covered entities are not required to agree to an individual/patient's request for a restriction, however, they are required to have policies in place by which to accept or deny such requests.
9. An individual/patient may not designate that some Confidential Health Information will be shared through NV-HIE, while other information will not. If an individual/patient specifies he/she does not wish to have particular Confidential Health Information shared through NV-HIE, all information on that patient will be blocked from view through NV-HIE.

10. Notwithstanding anything to the contrary set forth in these Policies and Procedures, Participants may disclose individual/patient demographic information to NV-HIE even if an individual/patient chooses not to participate in NV-HIE.
11. An individual/patient who has opted out of having his or her Health Information available through NV-HIE may choose at a later time to have his or her Health Information shared in NV-HIE, the individual/patient (or that individual's/patient's representative) must request, in a form or manner determined by the Participant, that the individual's/patient's Health Information be updated to reflect new status made available through NV-HIE. If an individual/patient chooses to participate in NV-HIE, all available information regarding the individual/patient may be accessed through NV-HIE.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

POLICY: Information Subject to Special Protection	EFFECTIVE: 12-21-2013
	REVISED:

PURPOSE

This policy promotes the privacy principles of purpose specification and minimization, security safeguards and controls, use limitation, data integrity and quality, collection limitation, and individual participation and control, particularly as it facilitates individualized privacy protections by requiring Participants to heed any special protections of certain information set forth under applicable laws. In complying with these special protections, Participants' collection, use and disclosure of health information is limited to legitimate purposes.

PROCESS

1. Some health information may be subject to special protection under federal, state, and/or local laws and regulations (e.g. substance abuse, mental health, and HIV).
2. Each Participant shall determine and identify what information is subject to special protection under applicable law prior to disclosing that information through NV-HIE.
3. Each Participant is responsible for complying with such laws and regulations.
4. Sensitive patient health information, (e.g. HIV/AIDS, sexually transmitted diseases, substance abuse, mental health conditions), that is shared with NV-HIE is still restricted from access for most purposes. This information can only be accessed with patient's consent and under an "opening the privacy seal" access process and only by a clinician.
5. Sensitive patient information is applied based on specific blocked codes. *Refer to Orion listing of protected codes for the specific blocked codes.* This applies to:
    i. Lab/Micro results (LOINC)
    ii. Medications (RxNorm)
    iii. Problems (ICD-9-CM)
    iv. Encounters (Diagnosis ICD-9-CM Code)
    v. Procedures (CPT codes)
6. The rules around who can see sensitive data:
    i. Level 1 Provider – Privacy Sealed Access only
    ii. All other users – No access.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

NEVADA HEALTH INFORMATION EXCHANGE

POLICY: NV-HIE Audit Policy	EFFECTIVE: 11-21-2013
	REVISED:

PURPOSE

To outline the process of performing periodic reviews and verifications of audit logs for both operational monitoring and system security and to ensure compliance with all applicable regulations and laws.

PROCESS

1. NV-HIE's IT Director or designee of NV-HIE is primarily responsible for execution and revision of the privacy and security policies, for ensuring audits occur by NV-HIE staff and that results and corrective actions are undertaken and reported as appropriate. The IT Director or his/her designee will oversee the activities of NV-HIE to evaluate compliance by Participants with this policy and enforce its terms.
2. An annual privacy and security internal audit plan will be developed by the IT Director or designee based on guidance from ONC and HIPAA regulations. This plan will receive input and direction from NV-HIE's HIT Advisory Council and NV-HIE's Board of Directors will be the governing body for final approval.
    a. The audit plan will include the types of audits to be performed, the specific controls to be audited and the frequency and sample size for each audit.
    b. Documentation of the audit and its results will be maintained and include the list of cases sampled for each audit, the audit schedule, and all audit activity.
3. Audit Process:
    a. Audits will be conducted on a statistically significant sample size.
    b. At least on an annual basis, or more frequently, as determined by the IT Director or designee, NV-HIE will generate a random sample of records to be audited and work with the Participants to establish a process for review to establish the following with respect to each such record:
        i. That any Authorized User who accessed Data of a Patient (1) executed the proper authorized user agreement and (2) had a treatment relationship with such Patient, or was authorized by the Participant to access such data.
4. Annually, the results of the privacy and security audits will be presented to the HIT Advisory Council for review and to NV-HIE's Board of Directors for final approval.
5. Participants will have the responsibility to ensure compliance with state and federal laws and regulations, such as HIPAA, to maintain the confidentiality, privacy and security of individuals' protected health information. This includes ensuring that NV-HIE is being used only for purposes authorized by the Participation Agreement, and that each individual who views data through NV-HIE is doing so in a manner consistent with state and federal laws and regulations and privacy and security policies.
6. The NV-HIE system will maintain audit trails. All user activity within the system is logged, enhancing audit capabilities and improving the general security of patient data. Audit trails

of user logins, logouts, applications used, security overrides, patient selections and individual documents viewed are recorded, with the date and time. Audit log data is stored in a separate audit database.

7. If an audit reveals noncompliance by a Participant, a corrective action plan must be submitted by the Participant to the NV-HIE IT Director or designee.
    a. The IT Director or designee will forward the matter to the NV-HIE Chief Executive Officer.
    b. The IT Director or his/her designee will make a recommendation on the corrective action plan to NV-HIE Chief Executive Officer as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Chief Executive Officer be rejected.
    c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Executive Director after obtaining advice of Legal Counsel may decide to suspend access to the Exchange for either the Participant or one or more Authorized Users of such Participant until the problem is adequately addressed.
8. If an audit reveals noncompliance by a NV-HIE staff, a corrective action plan must be submitted to the NV-HIE IT Director or designee.
    a. The IT Director or designee will forward the matter to the NV-HIE Chief Executive Officer.
    b. The IT Director or his/her designee will make a recommendation on the corrective action plan to NV-HIE Chief Executive Officer as to whether a specified corrective action plan should be accepted as presented, be revised as per agreement reached by the Chief Executive Officer or be rejected.
    c. If a corrective action plan is rejected, depending on the nature of the problem uncovered in the audit, the Executive Director after obtaining advice of Legal Counsel may choose to take necessary disciplinary action against the employee and suspend access to the Exchange for the employee until the problem is adequately addressed.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

NEVADA HEALTH INFORMATION EXCHANGE

POLICY: Enterprise Master Patient/Person Index Maintenance	EFFECTIVE: 11-21-2013
	REVISED:

PURPOSE

To ensure a process is implemented and followed to maintain the Enterprise Master Patient/Person Index (EMPI) and perform all duties necessary for ensuring the integrity and quality of the EMPI data.

PROCESS

1. Patient Matching
    a. NV-HIE, in conjunction with the EMPI Software vendor, will establish the matching thresholds to be used. These thresholds, along with industry standard matching algorithms, are used to identify the incoming and existing records that should be linked. NV-HIE staff will monitor the matching results, and make periodic adjustments to the thresholds as necessary.
    b. The EMPI Software vendor utilizes a proprietary algorithm to assess the similarity of individual records. When two records are compared, the algorithm generates a weighting that describes how similar the two records are. If this weighting falls below a Duplicate Threshold level, the records are treated as separate and no further actions are taken. If the weighting falls between the Duplicate Threshold and the Match Threshold, the system flags these records as being potential duplicates, and requires further manual intervention. If the weighting falls above the Match Threshold, the system automatically merges the two records, unless the records are flagged as potential false positives by the system, requiring further manual intervention. An example of a potential false positive is where two records are almost identical (as in the case of twins) resulting in a high weighting score, but the two records should remain unique. The algorithm considers certain demographic fields contained in a record - such as First Name, Last Name, Social Security Number, Date of Birth, Gender, etc. - and applies a weighting corresponding to how similar the two fields are to each other. Specific information regarding the Duplicate and Match Thresholds, field weightings, and other algorithm and matching-specific information can be found in the NV-HIE EMPI Settings document.
2. Unresolved Matches
    a. NV-HIE, in conjunction with Participants' HIM Director (or their designee), will establish procedures to correct any unresolved matches or discrepancies within the EMPI. Timeframes for resolution will be agreed to by all parties involved in establishing the procedure. The procedure and timeline for resolution will be reviewed periodically, and adjusted as necessary.
3. Access to EMPI
    a. NV-HIE's IT Director, or designee, must authorize access to the EMPI System. Direct access to the EMPI System will be granted to staff members, sub-contractors, EMPI software vendor, etc. as necessary to maintain the quality and integrity of the EMPI.

Additional access will have to be approved by the IT Director or their designee. The IT Director will periodically review the list of authorized users and remove users who will no longer be requiring access to maintain the EMPI.

4. Matching Process Audit
    a. NV-HIE will periodically perform audits on a sample set of records after they have been processed by the matching algorithm within the EMPI. This sample set will be compared to established matching thresholds to confirm the algorithm is functioning as configured.
5. Accuracy Threshold
    a. NV-HIE will implement processes to ensure an accuracy threshold of at least 95% is achieved in patient matching approach.

APPROVAL:

_____
Signature

_____
Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

NEVADA HEALTH INFORMATION EXCHANGE

POLICY: NV-HIE Training Policy	EFFECTIVE: 11-14-2013
	REVISED:

PURPOSE

To outline the process used by NV-HIE and its Participants in the training of Participants and its Authorized Users.

PROCESS

1. **General Purpose of Training:**
    a. The general purpose of the NV-HIE training is to assure that in building and operating NV-HIE, the focus is maintained on the welfare, safety and concerns of the patients.
    b. All users must be very aware of patient privacy and confidentiality concerns along with being thoroughly trained in the appropriate use of NV-HIE.
    c. NV-HIE only allows individuals who are trained as part of the NV-HIE training program to qualify as Authorized Users to access clinical data through NV-HIE or even for the limited purpose of entering status and/or demographic information into NV-HIE.
    d. Participating organizations are responsible for training all of its Authorized Users on compliance with applicable HIPAA regulations, privacy laws and rules and the Participant's privacy and security policies.
2. **Training Program:**
    a. The IT Director or designee shall develop and maintain the training materials for usage of NV-HIE.
    b. A train-the-trainer model is used with each Participant as part of the Onboarding Process. Each Participant shall determine those individuals designated as the "super users" or training program administrator for training purposes.
    c. Each Participant shall coordinate the training of designated individuals and for implementing the training.
    d. Each Participant will be responsible for assuring that all individuals that are designated as Authorized Users have the proper authorization and followed the Participant's protocol for Authorized Users access.
3. **Training of Authorized Users:**
    a. As noted above, each Participant will designate their "super users" who will be responsible for deploying training for all of its Authorized Users.
    b. NV-HIE staff and support personnel will offer assistance for this training on an as needed basis.
    c. Each Participant shall maintain the documentation of who has been designated as an Authorized User and their training.

NEVADA HEALTH INFORMATION EXCHANGE

APPROVAL:

_____
Signature

_____
Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

NEVADA HEALTH INFORMATION EXCHANGE

POLICY: Openness and Transparency Policy for Individually Identifiable Health Information	EFFECTIVE: 11-21-2013
	REVISED:

PURPOSE

To ensure an openness and transparency about policies, procedures, and technologies that directly affects individuals and/or their individually identifiable health information.

PROCESS

1. Participating organizations, as required by the HIPAA Privacy Rule, must provide a notice of its privacy practices (NPP) to patients, with certain exceptions. This notice of privacy practice should describe how PHI is collected, how it is used, and to whom and for what reason(s) it is disclosed, including the disclosure to a health information exchange. The notice should be:
    a. Simple, understandable, and at an appropriate literacy level.
    b. Highlight, through layering or other techniques the disclosures and uses that are most relevant (for example, the notice of privacy practice could have a summary sheet followed by a description of actual use and disclosure practices).
    c. Adhere to obligations for use of appropriate language(s) and accessibility to people with disabilities.
2. NV-HIE has no direct or indirect contact with patients, and thus requires that the duty of providing this notice belong to participating organizations.
3. Individuals should be able to understand what individually identifiable health information exists about them, how that individually identifiable health information is collected, used, and disclosed and whether and how they can exercise choice over such collections, uses, and disclosures.
4. Persons and entities, that participate in NV-HIE for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format.
5. Notice of policies, procedures, and technology-- including what information will be provided under what circumstances -- should be timely and, wherever possible, made in advance of the collection, use, and/or disclosure of individually identifiable health information.
6. Policies and procedures developed are consistent with the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information and should be communicated in a manner that is appropriate and understandable to individuals.
7. NV-HIE considers PHI to be information that identifies a patient, provided to a participating organization in the Exchange, and can include and includes any part of an individual's medical record or payment history.
8. NV-HIE mirrors the definition of protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually

Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E, and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C, both as amended from time to time.

9. As a conduit for the exchange of information among Participants, NV-HIE does not dictate the type of PHI the Participants collect and share with NV-HIE. NV-HIE's hybrid infrastructure model will store a minimum amount of health data centrally, primarily facilitating the secure transfer of health data among Participants that store the health data at their disparate locations. NV-HIE will enable the exchange of data stored in existing provider networks while maintaining an option to store data centrally (e.g., smaller provider groups without their own database or network; or public health surveillance databases).
10. As part of their policies, Participants must ensure that patients fully understand the nature of the information exchange, and a public relations effort may be required. At a minimum, these topics should be included in the NPP that each patient receives.
    a. Explain why Participants collect PHI.
    b. Describing the privacy practices and security safeguards for controlling PHI.
    c. Disclosing standards, guidelines, regulations and applicable laws regarding PHI.
    d. Disclosing who has access to PHI and why.
    e. Providing processes for patient redress.
    f. Identifying a primary point of contact and/or responsible party for PHI.
    g. Informing patients of their rights under the privacy policy.
    h. Providing patient options regarding the collection, use and disclosure of their PHI.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

NEVADA HEALTH INFORMATION EXCHANGE

POLICY: Participation Requirements for NV-HIE	EFFECTIVE: 11-21-2013
	REVISED:

PURPOSE

To provide guidelines defining the mandatory participation requirements as it relates to the Nevada Health Information Exchange (NV-HIE) and to outline the process used to onboard Participants onto NV-HIE.

PROCESS

1. Prior to accessing or making clinical data accessible through NV-HIE, each Participant must sign:
    a. The Participation Agreement
    b. The Business Associates Agreement
2. The IT Director or his/her designee is responsible for assuring that each Participant has executed a Participation Agreement prior to participating in the Exchange and/or exchanging Data.
3. As part of the onboarding process, the Participant will provide NV-HIE with:
    a. All the necessary contact information, i.e. Privacy/Security Officer, IT contact, Participation Agreement contact, etc.
    b. Completed Readiness Questionnaire
    c. Ensure that all Authorized Users have been properly assigned and documentation acquired.
4. Each Participant will provide system support services necessary for activities related to sharing and viewing data using NV-HIE, and for maintaining hardware used in connection with NV-HIE.
5. Each Participant is responsible for:
    a. Maintaining internet connectivity and for the performance of NV-HIE as limited by that connectivity.
    b. Cooperating with NV-HIE's staff or support personnel in troubleshooting any difficulties experienced by Authorized Users with respect to access and performance of NV-HIE.
    c. Cooperating with NV-HIE and its vendors in testing and implementing the system and any upgrades to NV-HIE.
6. Participants that contribute Data to NV-HIE are responsible for:
    a. Monitoring Data Exchanges from its systems to NV-HIE's Clinical Data Repository and solving any problems that may arise with respect to such Data Exchanges, ensuring accurate and complete loading of clinical Data from its legacy systems to the Clinical Data Repository. The Participant must notify NV-HIE of any problems in the regular Data Exchange to the Clinical Data Repository.
    b. Ensuring that processes are in place so that the impact on the Clinical Data Repository and NV-HIE of any changes to the legacy systems or operating environment are evaluated and tested, as necessary. The Participant must notify NV-HIE in advance of any system changes that will require an update to the Clinical Data Repository so that NV-HIE can participate in modification and/or testing procedures.
    c. Monitoring the VPN connectivity and coordinating with NV-HIE support services in accordance with the escalation process developed by the IT Director or his/her designee as necessary to troubleshoot and resolve any problems or issues.

NEVADA HEALTH INFORMATION EXCHANGE

APPROVAL:

_____
Signature

_____
Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

Nevada Health Information Exchange

POLICY: Notice of Privacy Practices	EFFECTIVE: 11-14-2013
	REVISED:

PURPOSE

To ensure each Participant has developed and maintained a notice of privacy practices (the Notice).

PROCESS

1. Each Participant shall develop and maintain a notice of privacy practices (the Notice). The Notice must describe the uses and disclosures of protected health information contemplated through the Participant's participation in the Health Information Exchange (NV-HIE).
2. The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule (45.C.F.R. § 164.520(b)) and comply with applicable laws and regulations.
3. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through the exchange. NV-HIE may provide sample language, such as noted below, for Participants upon their request:
    a. *We may make your protected health information available electronically through an electronic health information exchange to other health care providers that request your information for their treatment and business operations. Participation in an electronic health information exchange also lets us see their information about you for our treatment and business operations.*
4. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgement of receipt by the individual (see 45 C.F.R. § 164.520(c)(2)(ii)), which policies and procedures shall comply with applicable laws and regulations.
5. Participants may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

Security Breach Response Protocol

Procedures for Responding to a Security Breach Involving Electronic Protected Health Information

TABLE OF CONTENTS

INTRODUCTION

The purpose of this Security Breach Response Protocol ("Protocol") is to establish formal documented procedures to be followed when NV-HIE becomes aware of instances of unauthorized access to or disclosure of, patients' protected health information ("PHI"), in accordance with applicable state and federal laws and NV-HIE's policies.

This Protocol describes a recommended process for responding to such incidents, the conditions whereby this process is invoked, the resources required, and the course of recommended action. The primary emphasis of activities described within this Protocol is the return to a normalized (secure) state as quickly as possible, while minimizing the impact to NV-HIE, NV-HIE's customers and to the individuals/patients. However the appropriate type of response will depend on the specific facts of each PHI disclosure incident and applicable federal and state laws, and thus the process recommended by this Protocol may have to be revised accordingly.

This Protocol establishes the Security Breach Response Team, which shall have the responsibility for the actions contained herein.

DEFINITIONS

1. **Protected Health Information (PHI):** as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), protected health information[1] is defined as health information, including demographic information collected from an individual, and:
   (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
   (2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
      (i) that identifies the individual; or
      (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

2. **Security Incident:** a Security Incident[2], as defined by HIPAA, means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. A Security Incident poses a threat to NV-HIE's or NV-HIE's customers' physical environment or information systems. Each Security Incident will be evaluated and assessed a risk score based on the threat, vulnerability and impact of the Incident (See Appendix).

   Examples of a Security Incident assessed as Low (score of 4 or less) may include, but are not limited to:
   a. Pings on a firewall;
   b. Malware;
   c. Denial-of-service attacks that do not result in a server taken off-line;
   d. Port scans;

[1] 45 C.F.R. 160.103
[2] 45 C.F.R. 164.304

e. Attempts to log on to a system or application, or enter a database with an invalid password or user name.

Examples of a Security Incident assessed as Medium (score of 5-6) may include, but are not limited to:

a. PHI sent to an unintended recipient;
b. An employee using another user's identification;
c. Unauthorized access to PHI by an employee;
d. Failure to comply with NV-HIE's privacy and security policies and procedures.

3. **Security Breach:** A Security Incident assessed as High (score of 7-8) or Severe (score of 9), will be considered a Security Breach, requiring activation of this Protocol.

Examples of a Security Breach may include, but are not limited to:

a. Intentional, unauthorized access to NV-HIE's customers' data with the intent to sell, transfer, use for commercial advantage, personal gain, or malicious harm;
b. Theft or loss of portable media (such as unencrypted laptops or USB sticks) containing electronic PHI;
c. Law enforcement investigations that involve NV-HIE's information or personnel that may impact NV-HIE's or NV-HIE's customers' information, systems, facilities or workforce;
d. A Security Incident that, although unintentional, has a substantial risk of harm to a high number of individuals.

PROCESS

1. Security Incident Reporting (LOW-MEDIUM RISK):

a. Security Incident (Low Risk): Unsuccessful Security Incidents, such as attempts to access, misuse, disclose, modify or destroy information or physical assets shall be logged and tracked by NV-HIE in accordance with NV-HIE's policies and procedures. The IT Director or his/her designee shall be responsible for reviewing such logs and taking appropriate actions.

b. Security Incident (Low – Medium Risk): Any employee, data owner or customer who believes that a successful Security Incident has occurred, shall immediately notify the IT Director upon becoming aware of such Security Incident.

2. The Chief Executive Officer or his/her designee will conduct an investigation, coordinate the investigation with stakeholders, as appropriate to the incident, including, but not limited to: Information Security, customers and business associates, Human Resources, and others, as appropriate. The Chief Executive Officer or his/her designee shall maintain written documentation of the Security Incident, such as a description of the incident, root cause of the incident, remediation actions taken, and corrective measures applied.

If, during the investigation, the Chief Executive Officer determines that a Security Breach has occurred, he/she will immediately activate the Security Breach Response Team.

3. Security Breach Response Team:

   a. Security Breach Response Team ("Team") Composition – The Chief Executive Officer, or his/her designee, will be responsible for activating the Security Breach Response Team. Depending on the circumstances of the Security Breach, the Team will be comprised of appropriate representatives from the organization and/or customer affected.

   b. Team Objectives – The Team will take all commercially reasonable steps to minimize the potential negative impact of the Security Breach and restore services to a normalized and secure state of operations as soon as possible. In addition, the Team will:
      i. Coordinate and oversee the response to a Security Breach in accordance with the requirements of state and federal laws and NV-HIE's policies;
      ii. Where appropriate or as required by law, inform the affected individuals and third parties of action that is recommended or required on their behalf;
      iii. Provide clear and timely communication to all interested parties.
      iv. Conduct a post-Security Breach review;
      v. Ensure appropriate actions are taken to prevent a recurrence;
      vi. Establish, maintain and document periodic Security Breach Response Protocol testing;
      vii. Review the Security Breach Response procedures at least annually and update as necessary.

4. Response to a Security Breach

   a. Activation of the Team - The Chief Executive Officer or his/her designee shall be responsible for activating the Team and providing an initial report to the Team and Executive Management.

      Note: The following procedures may repeat or be concurrent depending upon the incident.

   b. Determination of the Risk - The Team will assess the risk to NV-HIE or NV-HIE's customer posed by the Security Breach by developing a risk assessment scoring tool (See Appendix) that is based on:

      - Threat (probability)
        - Malicious – intentional, targeted at NV-HIE
        - Inadvertent – untargeted threat

      - Impact (criticality)
        - Determine the potential damage and business impact of the incident
        - Determine if the incident has or will affect businesses or resources outside of the NV-HIE network

      - Vulnerability (exposure)
        - Determine if the incident is localized in nature or company wide

c. Communications and Notifications - The Chief Executive Officer will coordinate all internal and external communications and notifications as appropriate to the circumstances, including, but not limited to:
   - State and/or federal law enforcement
   - Regulators
   - Media
   - Customers, vendors and clients
   - Employees

   In addition:
   - Only the designated spokesperson, i.e., the Chief Executive Officer, or his/her designee, shall speak directly with the media;
   - All notifications will be documented, including date and time of notification, who was notified and who made the notification;
   - All communications pertaining to a Security Breach must be on a confidential, need-to-know basis;
   - The Chief Executive Officer shall monitor and communicate ongoing progress of the Security Breach investigation.

d. Recording the Incident – The Chief Executive Officer or his/her designee shall securely maintain all documentation relating to the Security Breach, including, but not limited to: a log of all activities and events in response to the Security Breach.

e. Ongoing Security Response Activities – during the course of the investigation, the Chief Executive Officer, or his/her designee, working with the Team may:
   i. Determine what additional parties need to be involved in the issue resolution;
   ii. Transfer some or all responsibility to the NV-HIE Incident Response Team (IRT) upon completion of the risk assessment. The IRT is under the direction of the Chief Executive Officer or his/her designee;
   iii. Identify and contact additional functional areas and/or individuals, as needed to respond.

5. Post-incident actions - The following actions will be initiated by the Chief Executive Officer and require involvement of the Team members or individuals, as appropriate:

   a. Meet with the Team and other appropriate individuals to assess the actual impact of the Security Breach;
   b. Lead efforts to determine root cause, if not already discovered;
   c. Designate responsibility for any follow-up security remediation activities to the appropriate business area/service line;
   d. Ensure that appropriate Security Breach notification is conducted to covered entities where NV-HIE is the business associate;
   e. Ensure each functional area has maintained chain of custody for collected evidence;

f. Identify and recommend the appropriate retroactive and prospective corrective actions to the Executive Committee;
g. Communicate final reporting to Executive Management, and others, as appropriate;
h. Declare the Security Breach response as completed;
i. Conduct "Lessons Learned" session(s);
j. Review/revise the Team procedures if needed;
k. Provide final report to Executive Management, the Executive Committee, and the Board of Directors.

APPENDIX

SECURITY RISK ASSESSMENT PROCESS

The Team will assess risk based on: (a) protecting the safety and personal well-being of the NV-HIE workforce and others; and (b) protecting the confidentiality, integrity, and availability of the NV-HIE information and information assets.

Risk will be assessed using the following three factors:

1. Threat – the likelihood (or actual event) that puts personnel or information resources at risk of harm, loss of confidentiality, integrity, or availability, or corruption of data;
2. Vulnerability – the exposure of personnel or information to potential threats;
3. Impact – the impact of the loss of information or personnel. This can be quantified in financial terms or qualified by importance to business operations (i.e., high, medium, or low.)

	Threat	Vulnerability	Impact
High	• An actual security breach has occurred or the probability of occurrence is extremely high (over 70%) • The nature of the threat is malicious in nature and cannot be effectively managed with existing controls • The threat is demonstrable and pervasive in the physical or computing environments	• Exposure to a particular threat is extremely high • Large volume of un-patched systems • Exposures that are easily gained • Large amount of data available in a particular facility	• Situation where personnel are at serious risk of harm • Financial impact of loss of data or system assets is significant • Security incident may cause significant embarrassment to NV-HIE, NV-HIE's customers, or individuals through media attention • Mitigation of vulnerability would be a serious impact to business operations • Significant operational impact resulting in the impact of critical business recovery time objectives • Estimated impact: over $500,000

Medium	• The probability of an actual security breach occurring is likely (30-70%) • The threat can be managed somewhat effectively with existing controls • The threat has been demonstrated to be effective against vulnerable systems – low number of incidents reported	• Exposure to a particular threat is moderate in scope • Measurable amount of information systems that are exposed • Access to systems, data, or personnel is moderately difficult to gain	• Financial impact of loss of data or system assets is measurable but not significant • Risk is not posed to PHI or other information assets of a confidential nature • Mitigation of vulnerability is not a significant impact to business operations • An incident that results in or is likely to result in significant impact to operations, including exceeding critical business unit maximum allowable delays • Estimated impact: Between $50,000-$500,000
	• The probability of an actual security breach occurring is low (less than 30%) • The threat can be managed effectively with existing controls • The threat is conceptual or perceived – no known incidents reported	• Exposure to a particular threat is low • Negligible amount of information systems that are exposed • Access to systems, data, or personnel is difficult to gain	• Financial impact of loss of data or system assets is not significant • Risk is not posed to sensitive information assets • Mitigation of vulnerability does not impact business operations • Minor data communications interruption • Estimated impact: Under $50,000

The Team must evaluate the security event using the above criteria as a guideline to determine the appropriate risk for each factor. A high-level risk posed against a low-level criticality may be determined to be of low-medium overall risk to NV-HIE.

The following procedure for evaluating the security event shall be used to determine if the event should be classified as a Security Incident or a Security Breach, and to drive the appropriate levels of response.

For each category (Threat, Vulnerability, Impact), the risk-level is scored as follows:

- **High** = 3 points
- **Medium** = 2 points
- **Low** – 1 point

EXAMPLE

	Threat	Vulnerability	Criticality	TOTAL
High	**3**			**3**
Medium		**2**	**2**	**4**
Low				**0**
TOTAL	**3**	**2**	**2**	**7**

Once each area is scored, total the values across the table, then down, to gain the Overall Risk Rating.

Each area will be assigned a score and the total will allow for ranking the risk:

- **SEVERE (or Critical if non-system related): 9 points**
- **HIGH: 7 - 8 points**
- **MEDIUM: 5 - 6 points**
- **LOW: 3 - 4 points**

NEVADA HEALTH INFORMATION EXCHANGE

POLICY: Security Breach Response Protocol	EFFECTIVE: 11-14-2013
	REVISED:

PURPOSE

To establish a Security Breach Response Protocol ("Protocol") for a NV-HIE employee to use as a resource upon becoming aware of an actual or possible security incident. The Protocol describes a recommended process for responding to such incidents, but recognizes that an appropriate type of response will depend on the specific facts of each incident and applicable federal and state laws.

RESPONSIBILITY

All NV-HIE employees involved in the access, use, release or disclosure of electronic protected health information ("ePHI").

DEFINITIONS

1. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of ePHI or interference with systems operations in an information system.

    a. An *attempted* or *unsuccessful* security incident means that there was no actual access, use, disclosure, etc. Examples of an attempted or unsuccessful security incident include, but are not limited to:
        i. Pings on a firewall;
        ii. Malware;
        iii. Denial-of-service attacks that do not result in a server taken off-line;
        iv. Port scans; and
        v. Attempts to log on to a system, application or database with an invalid password or user name.

    b. A *successful* security incident means that there was actual unauthorized access, use, disclosure, etc. Examples of a successful security incident include, but are not limited to:
        i. ePHI sent to an unintended recipient;
        ii. An employee using another user's identification to access ePHI;
        iii. Unauthorized access by an employee; and
        iv. Failure to comply with NV-HIE's privacy and security policies and procedures.

2. A security breach is a successful security incident that has been assessed as having a high or severe threat of harm, vulnerability or impact to NV-HIE or NV-HIE's customers. The Chief Executive Officer and/or the IT Director in concert with Legal Counsel will assess the security incident to determine the risk level.

PROCESS

1. NV-HIE has developed a Security Breach Response Protocol (see attached) that may be used as a resource to guide employees that become aware of a possible or actual successful security incident involving the ePHI of NV-HIE or of a NV-HIE customer.

2. Attempted or unsuccessful security incidents should be reported as soon as possible to NV-HIE's IT Director or his/her designee.

3. Successful security incidents should be reported immediately to NV-HIE's IT Director or his/her designee.

APPROVAL:

_____
Signature

_____
Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

NEVADA HEALTH INFORMATION EXCHANGE

POLICY: Physical security of hardware, data, media and equipment	EFFECTIVE: 11-14-2013
	REVISED:

PURPOSE

To facilitate compliance with all applicable laws and regulations regarding the system security, including, at a minimum (a) meeting the standards established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) pertaining to system security and workstation security and (b) complying with the security provisions of this Policy Manual with respect to the hardware and systems used by the Nevada Health Information Exchange (NV-HIE)

RESPONSIBILITY

NV-HIE's IT Director or his/her designee shall act as the Security Officer and ensure that NV-HIE complies with all applicable laws and regulations regarding the system security and physical security of the hardware, data, media and equipment utilized by the Nevada Health Information Exchange.

Participants of NV-HIE shall comply with all applicable laws and regulations regarding system security, including at a minimum, (a) meeting the standards established by HIPAA pertaining to system security and workstation security and (b) maintaining the security of the workstations through which their Authorized Users access NV-HIE.

NV-HIE's IT Director or his/her designee shall ensure that the Exchange's (NV-HIE's) technology vendor maintains the security of the hardware located in the vendor's data center (the "Data Center") as well as the hardware maintained by NV-HIE staff, i.e. laptops.

PROCESS

1. NV-HIE, Participants and all vendors will comply with, the following system security standards:
    a. To protect the confidentiality, integrity and availability of NV-HIE by taking the reasonable steps to protect hardware used in connection with NV-HIE, as well as the facilities in which it is located, from unauthorized physical access, tampering and theft.
    b. To physically locate hardware used in connection with NV-HIE in locations where physical access can be controlled in order to minimize the risk of unauthorized access.
    c. To take reasonable steps to ensure that the perimeter of facilities containing hardware used in connection with NV-HIE is physically sound, the external walls are properly constructed and the external doors have the appropriate protections against unauthorized access.
    d. To prevent against unauthorized access to the facilities at which hardware used in connection with NV-HIE is located by ensuring that doors and windows of all facilities are locked when unattended and that external protections, such as window guards or bars, are installed on all windows at ground level and any other windows as reasonably necessary to prevent unauthorized entry.
    e. To establish and document detailed rules to determine which workforce members are granted physical access rights to specific areas where hardware used in connection with NV-HIE is maintained and to provide such physical access rights to the work area only to

workforce members having a need for access to such an area in order to complete job responsibilities.

2. Data Center Security Standards
    a. To use the following controls at all delivery and loading areas to prevent unauthorized access to its facilities:
        i. Restrict access to a holding area from outside building to identified and authorized workforce members
        ii. Design the holding area so supplies can be unloaded without the delivery staff gaining access to other areas of the building.
        iii. Secure the external doors of the holding area when the internal door of the area is open.
    b. To take reasonable steps to ensure that the level of protection provided for NV-HIE, as well as the facilities in which they are housed, is commensurate with that of the identified threats and risks to the security of NV-HIE and its facilities.
3. Periodic risk analysis will be performed by NV-HIE's IT Director or his/her designee in order to assess the level of physical access risk and adjust procedures accordingly.
4. NV-HIE's staff laptops are prohibited from containing encrypted nor unencrypted PHI on the hard drive.

APPROVAL:

_____
Signature

_____
Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange

Nevada Health Information Exchange

POLICY: User Permissions Policy	EFFECTIVE: 11-21-2013
	REVISED:

PURPOSE

Patient privacy policies have been enabled by the Orion Health platform to control access to patients protected health information. This access is based on the following:

- The user's relationship with the patient
- The patient's opt-in status

PROCESS

1. **Access descriptions:**
   - No Access – the patient's name will not be visible to the user in a work list or list of search results.
   - Locked – the patient's name (demographic information) will be visible in a list of search results, but cannot be selected.
   - Privacy sealed – the patient's name will be visible and can be selected, but a reason for access will be required before the patient can be placed in context and their medical details viewed.
   - Full Access – clinical users have unrestricted access to clinical data/documents in the patient's medical record as they have a valid relationship with the patient and the patient has "opted-in", i.e. chosen to have their information available in the HIE.
2. **Providing an access reason is referred to as "Opening the privacy seal".**
   - Once this has been done, the user will be able to access that patient's record for a limited period of time without having to reapply the reason.
   - This time is configurable (as a single global variable for the whole solution) and the default is 12 hours. If the clinical user ends his/her Portal session, all open privacy seal access is ended and he or she will need to re-supply the reason for viewing the restricted information.
   - List of reasons for when the user "breaks the glass" and a comment field for free text for each.
3. **List of reasons for when the user 'breaks the glass':**
   - Direct patient care - clinician or primary care provider
   - Direct patient care – consultant
   - Direct patient care – emergency
   - Direct patient care-clinician requested
4. **Provider-patient relationships** are established via HL7 ADT messages from the participants EHR/registration systems. These include admitting physician, attending physician, primary care physician, referring physician.

5. **Data access rules:**
   - Sensitive patient information is applied based on specific blocked codes. This applies to:
     - Lab/Micro results (LOINC)
     - Medications (RxNorm)
     - Problems (ICD-9-CM)
     - Encounters (Diagnosis ICD-9-CM Code)
     - Procedures (CPT codes)
   - The rules around who can see sensitive data:
     - Level 1 Provider – Privacy Sealed Access only
     - All other users – No access.
6. Each Participant and NV-HIE shall have an **authorization process in** place to ensure users have access to only those applications and the protected health information that they are allowed to use or review.

APPROVAL:

_____

Signature

_____

Date

David LaBarge
Chief Executive Officer
Nevada Health Information Exchange