DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Nevada – Notice Regarding Privacy of Personally Identifiable Information Collected on the Internet from Consumers and Security of Information Maintained by a Data Collector and Other Businesses
PAGE: 1 of 10	**REPLACES POLICY DATED:** 10/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.DP.NV.003
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated legal entities in the state of Nevada, including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers, home health agencies, hospice agencies, and corporate departments, Groups, Divisions and Market (collectively Nevada Affiliates) that meet the definition of "Operator" in N.R.S. 603A.330 and/or meets the definition of "Data Collector" in N.R.S. 603A.030.

PURPOSE: To establish the requirements for each Company-affiliated legal entity to post an online Notice regarding Covered Information collected by Operator as required by N.R.S. 603A.340. The online Notice will include a statement informing Consumers of their right to opt-out of the Sale of their Covered Information. To establish the requirements for each Company-affiliated legal entity to provide a Designated Request Address through which Consumers may submit Verified Requests to opt-out of the Sale of their Covered Information.

Also to establish the requirements for the security of information maintained by Data Collectors and other businesses when there has been a breach of the security of the system data as set forth in N.R.S 603A.010 to 603A.290.

POLICY: All Operators of an Internet website or online service are responsible for the protection of Covered Information. This Policy sets forth the areas in which appropriate actions must be taken to ensure the use of Covered Information is limited and protected. An Operator of an Internet website or online service that collects certain items of personally identifiable information about Consumers in Nevada must make available a notice, that is located in the online Privacy Policy, containing certain information relating to the privacy of Covered Information collected by the Operator including a statement informing Consumers of their right to opt-out of the Sale of their Covered Information. Operators of an Internet website or online service that collects certain information from Consumers in Nevada are prohibited from making any Sale of certain information about a Consumer if so directed by the Consumer.

All required revisions to the online Privacy Policy will be drafted by the Corporate Information Protection and Security Department and inserted by resources such as the Corporate Information Technology Group or Division Marketing leadership, as applicable. Consumer requests will be routed to resources such as a Contact Center via the toll-free number provided in the online Privacy Policy. Identified resources at that location will forward Consumer requests to business owners such as the Corporate Marketing Department or Division Marketing leadership, as needed, for resolution. Generally, facilities will not receive or process Consumer requests.

EXCEPTION: Among other exceptions, the definition of Operator does not include an entity that is subject to the provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and the regulations adopted pursuant thereto.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Nevada – Notice Regarding Privacy of Personally Identifiable Information Collected on the Internet from Consumers and Security of Information Maintained by a Data Collector and Other Businesses
PAGE: 2 of 10	**REPLACES POLICY DATED:** 10/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.DP.NV.003
APPROVED BY: Ethics and Compliance Policy Committee	

DATA COLLECTOR

Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in this policy, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data. Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The requirements in this policy are in addition to, and not in the place of, any requirements under Health Information Portability and Accountability Act (HIPAA) and any and all other Federal laws, regulations and interpretive guidelines, and Facility policies promulgated thereunder.

PROCEDURE:

A. **Online Notice to Consumers:**
An Operator shall post an online notice that is accessible to Consumers. The notice shall:

1. Identify the categories of Covered Information that the Operator collects through its Internet website or online service about Consumers who use or visit the Internet website or online service and the categories of third parties with whom the Operator may share such Covered Information;
2. Provide a description of the process, if any such process exists, for an individual Consumer who uses or visits the Internet website or online service to review and request changes to any of his or her Covered Information that is collected through the Internet website or online service;
3. Describe the process by which the Operator notifies Consumers who use or visit the Internet website or online service of material changes to the notice;
4. Disclose whether a third party may collect Covered Information about an individual Consumer's online activities over time and across different Internet websites or online services when the Consumer uses the Internet website or online service of the Operator; and
5. State the effective date of the notice.

An Operator may remedy any failure to comply with the provisions above within 30 days after being informed of such a failure.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Nevada – Notice Regarding Privacy of Personally Identifiable Information Collected on the Internet from Consumers and Security of Information Maintained by a Data Collector and Other Businesses
PAGE: 3 of 10	**REPLACES POLICY DATED:** 10/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.DP.NV.003
APPROVED BY: Ethics and Compliance Policy Committee	

An Operator violates this requirement if the Operator:

- Knowingly and willfully fails to remedy a failure to comply with these provisions within 30 days after being informed of such a failure; or
- Makes available a notice that contains information that constitutes a knowing and material misrepresentation or omission that is likely to mislead a Consumer acting reasonably under the circumstances, to the detriment of the Consumer.

B. **Consumer Opt-Out Requests:**

1. An Operator shall establish a Designated Request Address through which a Consumer may submit a Verified Request.
2. A Consumer may, at any time, submit a Verified Request through the Designated Request Address to an Operator directing the Operator not to make any Sale of any Covered Information the Operator has collected or will collect about the Consumer.
3. An Operator that has received a Verified Request submitted by a Consumer shall not make any Sale of any Covered Information the Operator has collected or will collect about that Consumer.

An Operator shall respond to a Verified Request submitted by a Consumer within 60 days after receipt of the request. An Operator may extend by not more than 30 days if the Operator determines that such an extension is reasonably necessary. An Operator that extends the period must notify the Consumer of such an extension.

C. **Security Measures**

A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce.

A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data

collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section.

The Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration shall create, maintain and make available to the public a list of controls and standards with which the State is required to comply pursuant to any federal law, regulation or framework that also satisfy the controls and standards set forth in subsection 2.

D. **Security Measure for data collector that accepts payment card**

1. If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization.
2. A data collector doing business in this State to whom subsection 1 does not apply shall not:
   a. Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or
   b. Move any data storage device containing personal information beyond the logical or physical controls of the data collector, its data storage contractor or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal information, unless the data collector uses encryption to ensure the security of the information.
3. A data collector shall not be liable for damages for a breach of the security of the system data if:
   a. The data collector is in compliance with this section; and
   b. The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents.
4. The requirements of this section do not apply to:
   a. A telecommunication provider acting solely in the role of conveying the communications of other persons, regardless of the mode of conveyance used, including, without limitation:
      i. Optical, wire line and wireless facilities;
      ii. Analog transmission; and
      iii. Digital subscriber line transmission, voice over Internet protocol and other digital transmission technology.
   b. Data transmission over a secure, private communication channel for:

i. Approval or processing of negotiable instruments, electronic fund transfers or similar payment methods; or
ii. Issuance of reports regarding account closures due to fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.

5. As used in this section:
   a. "Data storage device" means any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives and optical computer drives, and the medium itself.
   b. "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using:
      i. An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data;
      ii. Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology; and
      iii. Any other technology or method identified by the Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration in regulations adopted pursuant to NRS 603A.217.
   c. "Facsimile" means an electronic transmission between two dedicated fax machines using Group 3 or Group 4 digital formats that conform to the International Telecommunications Union T.4 or T.38 standards or computer modems that conform to the International Telecommunications Union T.31 or T.32 standards. The term does not include onward transmission to a third device after protocol conversion, including, but not limited to, any data storage device.
   d. "Multifunctional device" means a machine that incorporates the functionality of devices, which may include, without limitation, a printer, copier, scanner, facsimile machine or electronic mail terminal, to provide for the centralized management, distribution or production of documents.
   e. "Payment card" has the meaning ascribed to it in NRS 205.602.
   f. "Telecommunication provider" has the meaning ascribed to it in NRS 704.027.

E. **Notification**

1. The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that the notification will not

compromise the investigation.

2. For the purpose of this section, except as otherwise provided in subsection C5, the notification required by this section may be provided by one of the following methods:
   a. Written notification.
   b. Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq.
   c. Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information. Substitute notification must consist of all the following:
      i. Notification by electronic mail when the data collector has electronic mail addresses for the subject persons.
      ii. Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website.
      iii. Notification to major statewide media.

3. A data collector which:
   a. Maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.
   b. Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section.

4. If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.

F. **Enforcement**

1. If the Attorney General has reason to believe that an Operator, either directly or indirectly, has violated or is violating the notice or opt-out requirements set forth above, the Attorney General may institute an appropriate legal proceeding against the Operator. The district court, upon a showing that the Operator, either directly or indirectly, has violated or is violating the notice or opt-out requirements set forth above, may:

a. Issue a temporary or permanent injunction; or
b. Impose a civil penalty not to exceed $5,000 for each violation.

There is no private right of action against an Operator.

2. Civil Action: A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification.

3. Restitution: In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the court may order a person who is convicted of unlawfully obtaining or benefiting from personal information obtained as a result of such breach to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the notification required pursuant to NRS 603A.220, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification.

4. Injunction: If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of NRS 603A.010 to 603A.290, inclusive, the Attorney General or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.

G. **Destruction**

1. A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records.

2. As used in this section:
   a. "Business" means a proprietorship, corporation, partnership, association, trust, unincorporated organization or other enterprise doing business in this State.
   b. "Reasonable measures to ensure the destruction" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:
      iv. Shredding of the record containing the personal information; or
      v. Erasing of the personal information from the records.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Nevada – Notice Regarding Privacy of Personally Identifiable Information Collected on the Internet from Consumers and Security of Information Maintained by a Data Collector and Other Businesses
PAGE: 8 of 10	**REPLACES POLICY DATED:** 10/1/19
EFFECTIVE DATE: December 1, 2021	**REFERENCE NUMBER:** IP.DP.NV.003
APPROVED BY: Ethics and Compliance Policy Committee	

DEFINITIONS

1. **"Breach of the security of the system data"** means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. The term does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.
2. **"Consumer"** means a person who seeks or acquires, by purchase or lease, any good, service, money or credit for personal, family or household purposes from the Internet website or online service of an Operator.
3. **"Covered Information"** means any one or more of the following items of personally identifiable information about a Consumer collected by an Operator through an Internet website or online service and maintained by the Operator in an accessible form:
   a. a first and last name;
   b. a home or other physical address which includes the name of a street and the name of a city or town;
   c. an electronic mail address;
   d. a telephone number;
   e. a social security number;
   f. an identifier that allows a specific person to be contacted either physically or online;
   g. any other information concerning a person collected from the person through the Internet website or online service of the Operator and maintained by the Operator in combination with an identifier in a form that makes the information personally identifiable.
4. **"Data collector"** means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with non-public personal information.

   A data collector who is also an operator, as defined in NRS 603A.330, shall comply with the provisions of NRS 603A.300 to 603A.360, inclusive.
5. **"Designated Request Address"** means an electronic mail address, toll-free telephone number or Internet website established by an Operator through which a Consumer may submit to an Operator a Verified Request.
6. **"Operator"** means a person who:
   a. Owns or operates an Internet website or online service for commercial purposes;
   b. Collects and maintains Covered Information from Consumers who reside in Nevada and use or visit the Internet website or online service; and
   c. Purposefully directs its activities toward Nevada, consummates some transaction with

Nevada or a resident thereof, purposefully avails itself of the privilege of conducting activities in Nevada or otherwise engages in any activity that constitutes sufficient nexus with Nevada to satisfy the requirements of the United States Constitution.

The term does not include, among other exceptions, an entity that is subject to the provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and the regulations adopted pursuant thereto.

7. **"Personal information"**
   a. Personal information means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:
      i. Social security number.
      ii. Driver's license number, driver authorization card number or identification card number.
      iii. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.
      iv. A medical identification number or a health insurance identification number.
      v. A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.
   b. The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.
8. **"Sale"** means the exchange of Covered Information for monetary consideration by the Operator to a person for the person to license or sell the Covered Information to additional persons. The term does not include:
   a. The disclosure of Covered Information by an Operator to a person who processes the Covered Information on behalf of the Operator;
   b. The disclosure of Covered Information by an Operator to a person with whom the Consumer has a direct relationship for the purposes of providing a product or service requested by the Consumer;
   c. The disclosure of Covered Information by an Operator to a person for purposes which are consistent with the reasonable expectations of a Consumer considering the context in which the Consumer provided the Covered Information to the Operator;
   d. The disclosure of Covered Information to a person who is an affiliate of the Operator. For the purposes of this definition, "affiliate" means any company that controls, is controlled by or is under common control with another company; or

e. The disclosure or transfer of Covered Information to a person as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the person assumes control of all or part of the assets of the Operator.

9. **"Verified Request"** means a request:
   a. Submitted by a Consumer to an Operator for the purposes of directing the Operator not to make any Sale of any Covered Information the Operator has collected or will collect about the Consumer; and
   b. For which an Operator can reasonably verify the authenticity of the request and the identity of the Consumer using commercially reasonable means.

REFERENCES:

1. Senate Bill 220; N.R.S. 603A.300 to 603A.360
2. N.R.S 603A.010 to 603A.290
3. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Standards for Notification in the Case of Breach of Unsecured Protected Health Information, 45 CFR Parts 160 and 164
4. Protected Health Information Breach Risk Assessment and Notification, IP.PRI.011
5. Records Management Policy, EC.014