CMS- UPDATE

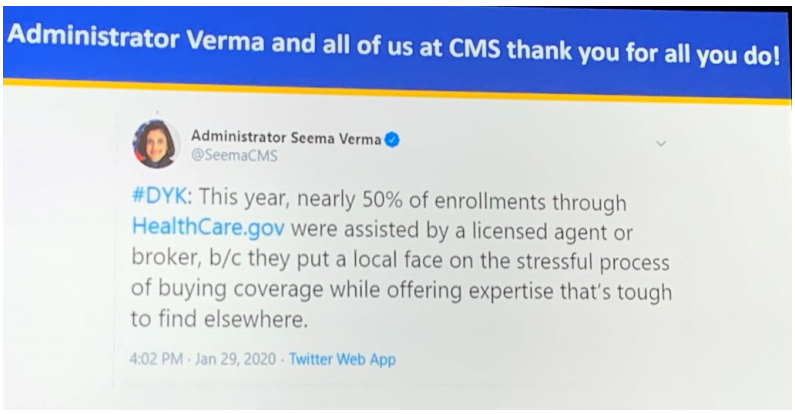
Randy Pate, CMS, CCIIO Director

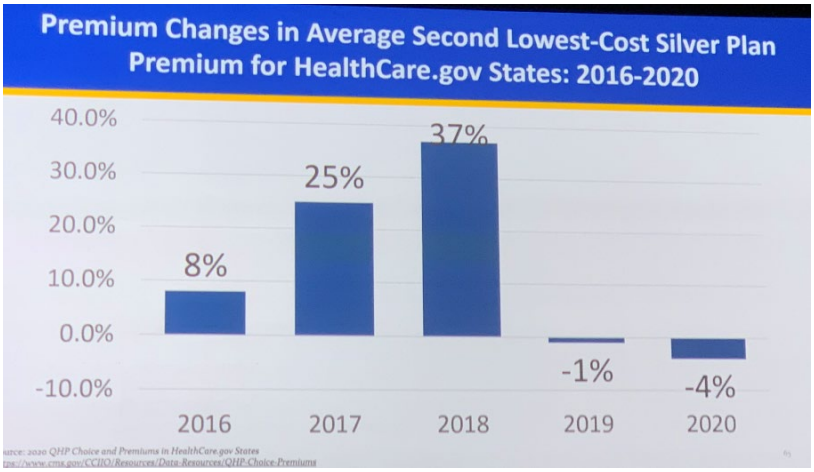
178,000,000 on Employer Group Plans
28,000,000 on Direct Purchase
58,000,000 on Medicare type plans
58,000,000 on Medicaid
11,000,000 on Exchange
3,000,000 on VA
27,000,000 Uninsured (7.4% of US Population)
363,000,000 US Population

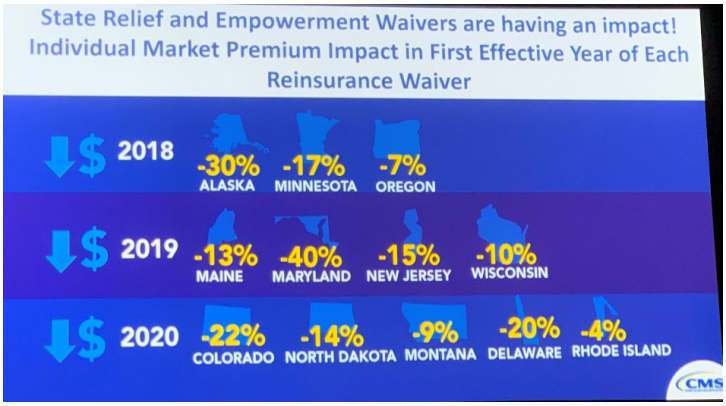
336,000,000 with Medical Insurance (92% have Medical Insurance)
206,000,000 or 61% Enrolled on Employer Plan or Direct Purchase
130,000,000 or 39% Enrolled in Government plans (Medicare, Medicaid, Exchange, VA)

Marketplace Update

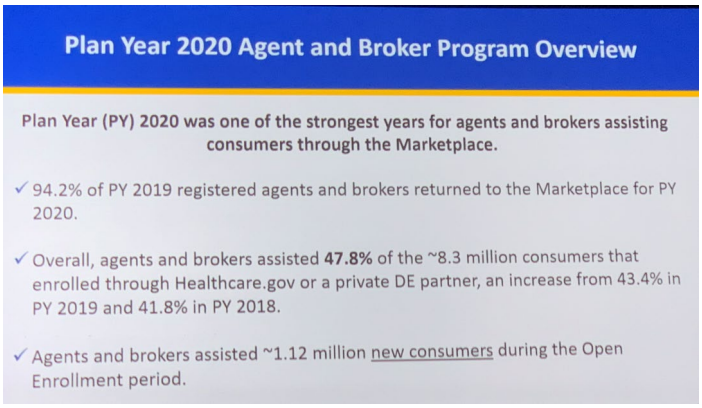
Seema Verma, Administrator for CMS

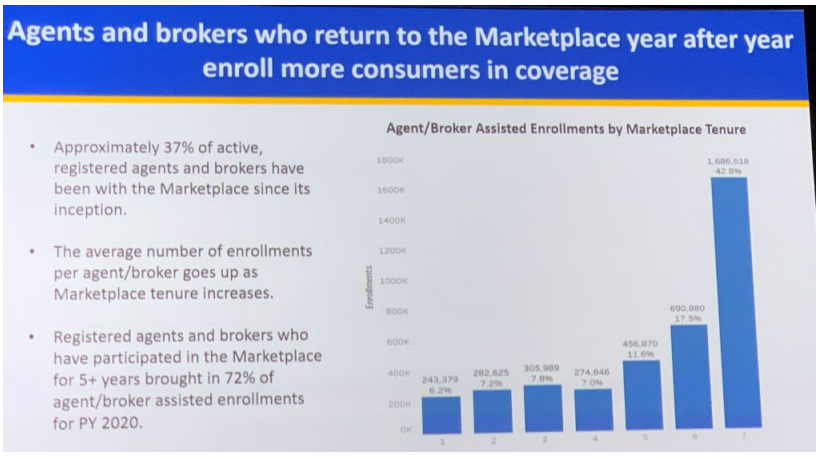






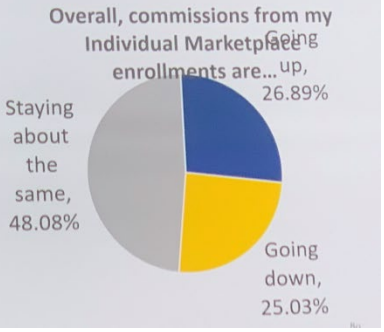
Section 1332 Waivers allows States to implement Invisible High-Risk Pools through Self-Funding





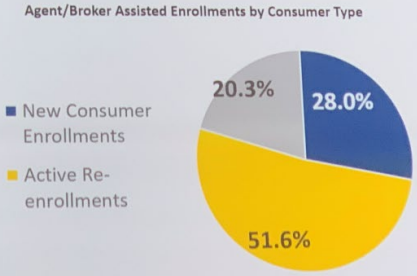
Agents and brokers are indicating that commissions have remained consistent, and may be heading up

- Based on the results of the PY 2020 Agent and Broker Post-Open Enrollment Feedback Questionnaire, the number of agents and brokers indicating they received commissions for the majority of their actively assisted enrollments has increased each year since 2017, reaching 69% for PY 2020.
- Overall, agents and brokers indicated commissions are remaining consistent, and we are hearing from industry leaders that commissions are likely heading up as the Marketplace continues to stabilize.

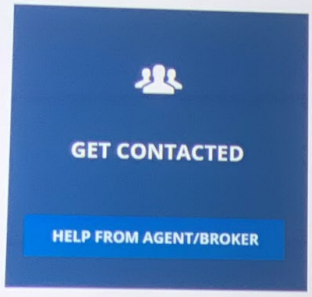


Agents and brokers actively assisted their clients and enrolled new customers at the highest levels this year

- Agent/broker assisted enrollments included the highest percentage of active enrollments (79.6%) and new enrollments (28.0%) to date.
- There were approximately 292,000 more active agent/broker assisted enrollments in PY 2020 than PY 2019.



Help On Demand continues to help agents and brokers expand their business with the Marketplace



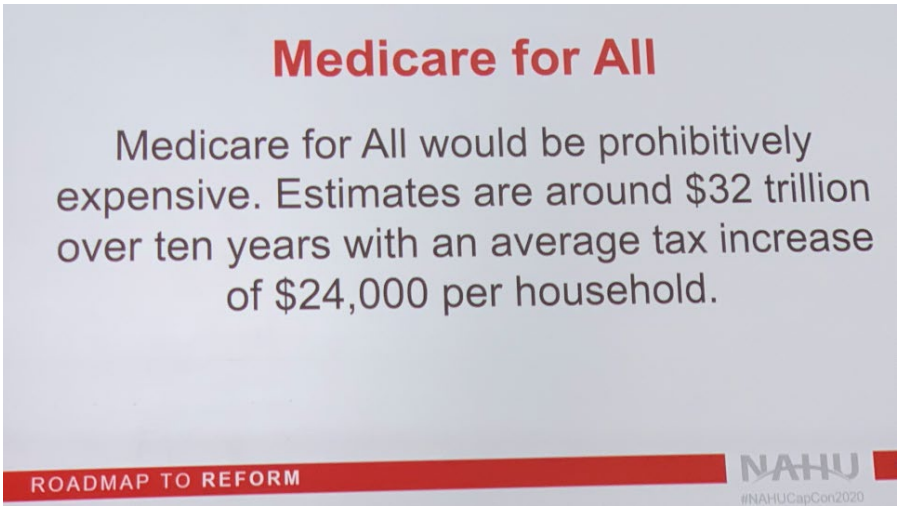
- Nearly 16% of all registered agents and brokers participated in Help On Demand for PY 2020, including 2,000 new agents or brokers who joined the program in 2019.
- Based on the results of the PY 2020 Help On Demand Feedback Questionnaire, 64% of agents and brokers felt Help On Demand expanded their ability to assist consumers for PY 2020, and nearly 87% of agents and brokers are likely to participate in Help On Demand for PY 2021.

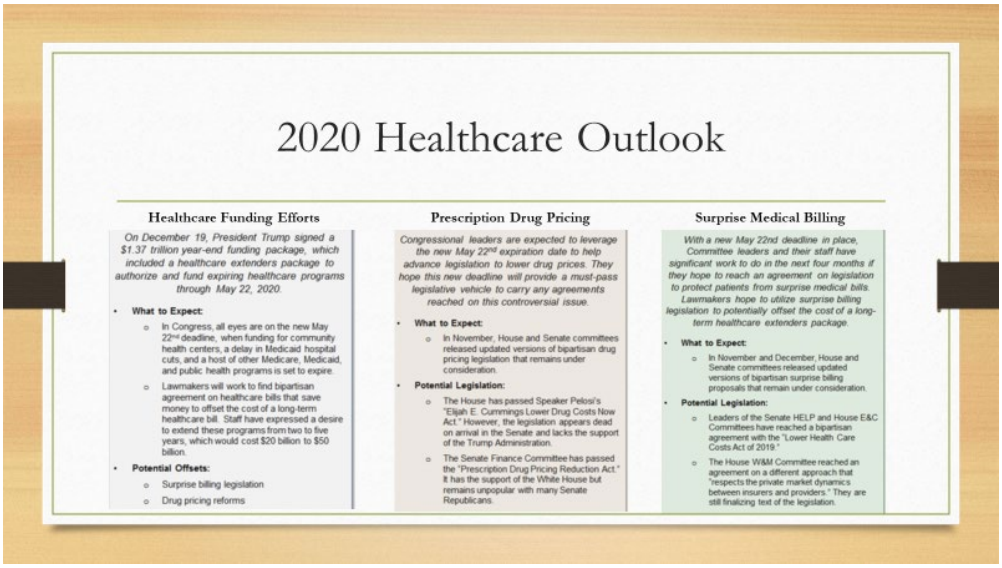
Looking Ahead

CCIIO continues to focus on stabilizing the market and making it easier for agents and brokers to enroll consumers in Marketplace coverage

- ✓ Continuing to stabilize the Marketplace with the goal of increasing issuer and plan availability, which may lead to increased commissions as carriers look to expand their footprint
- ✓ Continuing to streamline the online application on HealthCare.gov
  - Updating the cancellation and termination functionality
  - Adding affordability calculations for Individual Coverage and Qualified Small Employer HRAs
- ✓ Improving EDE functionality and adding new approved partners that work with agents and brokers
- ✓ Supporting complex consumer enrollments and SEPs through the Complex Case Help Center
- ✓ Making it easier for consumers to connect with agents and brokers through Help On Demand
- ✓ Promoting the adoption of Individual Coverage Health Reimbursement Arrangements (ICHRAs) to deliver more health coverage choices for employers and employees

NAHU Medicare UPDATE





Employer Exclusion

The employer-based system is highly efficient at providing American workers and their families with affordable coverage options through group purchasing and its associated economies of scale by spreading risk and avoiding adverse selection.

The success of this system is possible because of the preferential tax treatment of employer-sponsored insurance coverage, where employer-paid contributions for an employee's health insurance are excluded from that employee's compensation for income and payroll tax purposes.

Proposals that would cap the maximum value of the exclusion or eliminate it altogether would be detrimental to the stability of the employer-based market and would negatively affect middle-class Americans who currently benefit from this provision.

Employer Reporting

Establish a new voluntary reporting system, reduce the number of individuals and amount of information that would need to be reported, and eliminate the requirement to collect dependent social security numbers.

H.R. 4070 | Reps. Mike Thompson (D-CA) and Adrian Smith (R-NE)
S. 2366 | Sens. Mark Warner (D-VA) and Rob Portman (R-OH)

Employee Flexibility Act

Restore the 40-Hour Workweek; Repeal the 30-hour threshold for full-time employee for purposes of the employer mandate in the ACA and replace it with 40 hours.

S. 1510 – Sens. Todd Young (R-IN) and Joe Manchin (D-WV)

H.R. 2782 – Reps Jackie Walorski (R-IN) and Dan Lipinski (D-IL)

COBRA

Treat COBRA coverage as creditable coverage for Medicare, the same way that similar employer-sponsored insurance is already treated as creditable.

H.R. 2564 | Reps. Kurt Schrader (D-OR) and Gus Bilirakis (R-FL)
TBD | Sen. Todd Young (R-IN) and Sherrod Brown (D-OH)

Balance/Surprise Billing

NAHU is committed to working with policymakers at both the federal and state levels to address the issue of surprise and balance medical bills. The NAHU Legislative Council's special Balance-Billing Work group is specifically tasked with identifying potential solutions and proposing them to policymakers.

S. 1895 | Lower Health Care Costs Act
Sens. Lamar Alexander (R-TN) and Patty Murray (D-WA)

H.R. 3630 | No Surprises Act
Reps. Frank Pallone (D-NJ) and Greg Walden (R-OR)

S. 1531 | **Stopping The Outrageous Practice of (STOP) Surprise Medical Bills Act**
(Arbitration)
Sens. Bill Cassidy, (R-LA), Michael Bennet (D-CO), Todd Young (R-IN), Maggie Hassan (D-NH), Lisa Murkowski (R-AK) and Tom Carper (D-DE)

Bipartisan Prescription Drug Efforts

H.R. 3, led by House Speaker Nancy Pelosi (D-CA), would authorize Medicare to negotiate drug prices, require drug makers to pay rebates for increasing prices beyond the rate of inflation (penalties starting at 65% of the manufacturer's annual gross sales of the drug, escalating by 10 percentage points every quarter of noncompliance to a maximum 95%), and limit out-of-pocket costs for Medicare beneficiaries.

- **HR 3** passed a Democrat controlled House in December 2019. However, the legislation appears dead on arrival in the Republican-controlled Senate and currently lacks the support of the Trump Administration.
- In response to **HR 3**, Senators Chuck Grassley (R-IA) and Ron Wyden (D-OR) passed the **"Prescription Drug Pricing Reduction Act"** through the Senate Finance Committee, which has the support of the White House, but continues to be unpopular among mainstream Senate Republicans.
  - The bill caps out-of-pocket costs for Medicare enrollees and requires drug makers to pay rebates if they hike prices faster than inflation.

Nevada Updates

Ryan High
Chief Operations Officer
Silver State Health Insurance Exchange

Nevada Numbers from Nevada Health Link

- We enrolled 77,410 consumers for PY2020
- Average net premium was ~ $281
- 80% of consumers were eligible for APTC
- 45,698 actively shopped
- 20,111 were new consumers
- Of active enrollees, 26,000 were broker designated enrollees
- 19,000 were self-service enrollees

SB21 Task Force will move forward to create the language for a proposed Cyber Liability bill to address the issue and to provide direction for producers enabling them to be compliant without unreasonable regulation and threats to their business.

In addition to the suspension or revocation of a license, certificate of authority or registration, after notice and a hearing held pursuant to NRS 679B.310 to 679B.370, inclusive, impose an administrative fine of not more than $1,000 per day for each violation or failure to comply with the provisions of this chapter, up to a maximum fine of $50,000.

AB469 Passed May 15th, 2019

Summary

AN ACT relating to health care; limiting the amount a provider of health care may charge a person who has health insurance for certain medically necessary emergency services provided when the provider is out-of-network; requiring an insurer to arrange for the transfer of a person who has health insurance to an in-network facility under certain circumstances; prescribing procedures for determining the amount that an insurer is required to pay a provider of health care which is out-of-network for certain medically necessary emergency services provided to an insured; requiring the reporting of certain information related to that process; and providing other matters properly relating thereto.

NEVADA REVISED STATUTES CHAPTER 603A:
SECURITY AND PRIVACY OF PERSONAL INFORMATION

SECURITY OF INFORMATION MAINTAINED BY DATA COLLECTORS AND OTHER BUSINESSES

General Provisions

NRS 603A.010. Definitions. As used in NRS 603A.010 to 603A.290, inclusive, unless the context otherwise requires, the words and terms defined in NRS 603A.020, 603A.030 and 603A.040 have the meanings ascribed to them in those sections.

(Added to NRS by 2005, 2503; A 2017, 4079)

NRS 603A.020. Breach of the security of the system data" defined. "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.

(Added to NRS by 2005, 2503)

NRS 603A.030. "Data collector" defined. "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 nonpublic personal information.

(Added to NRS by 2005, 2504)

NRS 603A.040. "Personal information" defined.

1. "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:
   (a) Social security number.
   (b) Driver's license number, driver authorization card number or identification card number.
   (c) 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.
   (d) A medical identification number or a health insurance identification number.
   (e) 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.
2. 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.

(Added to NRS by 2005, 2504; A 2005, 22nd Special Session, 109; 2007, 1314; 2011, 2411; 2015, 241)

Applicability

NRS 603A.100. Applicability; waiver of provisions prohibited.

1. The provisions of NRS 603A.010 to 603A.290, inclusive, do not apply to the maintenance or transmittal of information in accordance with NRS 439.581 to 439.595, inclusive, and the regulations adopted pursuant thereto.
2. 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.
3. Any waiver of the provisions of NRS 603A.010 to 603A.290, inclusive, is contrary to public policy, void and unenforceable.

(Added to NRS by 2005, 2506; A 2011, 1762; 2017, 4079)

Regulation of Business Practices

NRS 603A.200. Destruction of certain records.

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:

(1) Shredding of the record containing the personal information; or

(2) Erasing of the personal information from the records.

(Added to NRS by 2005, 2504)

NRS 603A.210. Security measures.

1. 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.

2. 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.

3. 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.

(Added to NRS by 2005, 2504)

NRS 603A.215. Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability.

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:

(1) Optical, wire line and wireless facilities;

(2) Analog transmission; and

(3) Digital subscriber line transmission, voice over Internet protocol and other digital transmission technology.

(b) Data transmission over a secure, private communication channel for:

(1) Approval or processing of negotiable instruments, electronic fund transfers or similar payment methods; or

(2) 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:

(1) 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;

(2) 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

(3) 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.

(Added to NRS by 2009, 1603; A 2011, 2002)

NRS 603A.217 Alternative methods of and technologies for encryption: Adoption of regulations. Upon receipt of a well-founded petition, the Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration may, pursuant to chapter 233B of NRS, adopt regulations which identify alternative methods or technologies which may be used to encrypt data pursuant to NRS 603A.215.

(Added to NRS by 2011, 2002)

NRS 603A.220. Disclosure of breach of security of system data; methods of disclosure.

1. 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 subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.

2. 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.

3. The notification required by this section 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.

4. For purposes of this section, except as otherwise provided in subsection 5, 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:

(1) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons.

(2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website.

(3) Notification to major statewide media.

5. 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.

6. 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.

(Added to NRS by 2005, 2504)

Remedies and Penalties

NRS 603A.270. 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.

(Added to NRS by 2005, 2506) — (Substituted in revision for NRS 603A.900)

NRS 603A.280 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.

(Added to NRS by 2005, 2506) — (Substituted in revision for NRS 603A.910)

NRS 603A.290 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.

(Added to NRS by 2005, 2506; A 2017, 4079) — (Substituted in revision for NRS 603A.920)

NEVADA ADMINISTRATIVE CODE 679B

NOTE: In September 2018, the Commissioner of Insurance adopted new data security-related requirements (as part of LCB File No. R125-18) that took effect on October 2018. The relevant portions of the new promulgated regulation follow below.

Section 1. Chapter 679B of NAC is hereby amended by adding thereto the provisions set forth as sections 2 to 10, inclusive, of this regulation.

Sec. 2. ***"Nonpublic personal health information" means health information:***
1. That identifies a person who is the subject of the information; or
2. With respect to which there is a reasonable basis to believe that the information could be used to identify a person.

Sec. 3. ***"Nonpublic personal information" means:***
1. Nonpublic personal financial information; and
2. Nonpublic personal health information.

Sec. 4. ***As used in sections 4 to 10, inclusive, of this regulation, unless the context otherwise requires, the words and terms defined in sections 5, 6 and 7 of this regulation have the meanings ascribed to them in those sections.***

Sec. 5. ***"Customer information" means nonpublic personal information about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.***

Sec. 6. ***"Customer information system" means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.***

Sec. 7. ***"Service provider" means a person who maintains, processes or is otherwise allowed access to customer information through the person's provision of services directly to the licensee.***

Sec. 8. ***Each licensee shall implement a comprehensive written program for the security of customer information. The program must include administrative, technical and physical safeguards for the protection of customer information. Such administrative, technical and physical safeguards must be appropriate for the size and complexity of the licensee and the nature and scope of the licensee's activities.***

Sec. 9. ***A program implemented pursuant to section 8 of this regulation for the security of customer information must be designed to:***
1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threat or hazard to the security and integrity of the customer information; and
3. Protect against unauthorized access to, or use of, the customer information that could result in substantial harm or inconvenience to a customer.

Sec. 10. ***To determine whether a program implemented pursuant to section 8 of this regulation is satisfactory, the Commissioner will consider:***
1. The manner in which, in order to assess risk, the licensee:
(a) Identifies reasonably foreseeable internal and external threats or hazards which could result in the unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;
(b) Assesses the likelihood and potential damage of the threats or hazards, taking into consideration the sensitivity of the customer information; and
(c) Assesses the sufficiency of policies, procedures, safeguards and customer information systems to manage and control risks.

2. Whether, in order to manage and control risk, the licensee:

(a) Designs such a program to control the identified risks, commensurate with the sensitivity of the customer information and the complexity and scope of the licensee's activities;

(b) Trains staff, as appropriate, to implement the program; and

(c) Regularly tests or monitors the key controls, systems and procedures of the program. The frequency and nature of such tests or monitoring practices must be determined by the risk assessment performed by the licensee.

3. Whether, in order to oversee arrangements with service providers, the licensee:

(a) Exercises due diligence in selecting service providers;

(b) Requires service providers to implement appropriate measures designed to meet the objectives of this section; and

(c) Takes appropriate steps to confirm that service providers have satisfied the requirements imposed pursuant to paragraph (b).

4. Whether the licensee monitors, evaluates and adjusts, as appropriate, such a program considering:

(a) Relevant changes in technology;

(b) Changes in customer information systems;

(c) The sensitivity of customer information;

(d) Internal and external threats or hazards to the customer information; and

(e) Changes in the business arrangements of the licensee, including, without limitation, mergers, acquisitions, alliances, joint ventures and outsourcing arrangements.

5. Any other information which the Commissioner deems relevant to the determination.