ALTERNATIVE(S) TO WHAT IS BEING REQUESTED/RECOMMENDED:

The proposed revisions will align the Board's policy with existing mandates of federal and state law; therefore, no alternatives have been brought forward.

POLICY PROPOSAL
TITLE 4, CHAPTER 1, SECTION 22 (in part)
Data Security

Additions appear in ***boldface italics***; deletions are [~~stricken~~ and bracketed]

7. Data Security Policy

NRS 239B.030 Recorded, filed or otherwise submitted documents. [Effective January 1, 2008.]

1. Except as otherwise provided in subsections 2 and 6, a person shall not include and a governmental agency shall not require a person to include any personal information about a person on any document that is recorded, filed or otherwise submitted to the governmental agency on or after January 1, 2007.

2. If personal information about a person is required to be included in a document that is recorded, filed or otherwise submitted to a governmental agency on or after January 1, 2007, pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant, a governmental agency shall ensure that the personal information is maintained in a confidential manner and may only disclose the personal information as required:

(a) To carry out a specific state or federal law; or

(b) For the administration of a public program or an application for a federal or state grant.

➥ Any action taken by a governmental agency pursuant to this subsection must not be construed as affecting the legality of the document.

3. A governmental agency shall take necessary measures to ensure that notice of the provisions of this section is provided to persons with whom it conducts business. Such notice may include, without limitation, posting notice in a conspicuous place in each of its offices.

4. A governmental agency may require a person who records, files or otherwise submits any document to the governmental agency to provide an affirmation that the document does not contain personal information about any person or, if the document contains any such personal information, identification of the specific law, public program or grant that requires the inclusion of the personal information. A governmental agency may refuse to record, file or otherwise accept a document which does not contain such an affirmation when required or any document which contains personal information about a person that is not required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant.

5. On or before January 1, 2017, each govem it6 o7e1(]7c 0.26.a(i)4at)4(ion a)83(u)-1(st)4(ate021 Tc 3(e)2(nt)4( )-m)13

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. "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:

1. Social security number.
2. Driver's license number or identification card number.
3. 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.

➥ The term does not include the last four digits of a social security number or publicly available information that is lawfully made available to the general public.

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

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. And5214 .r4(.)1 Tc(o)5(nt)4 os

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