

**NEVADA SYSTEM OF HIGHER EDUCATION
PROCEDURES AND GUIDELINES MANUAL**

CHAPTER 4

GENERAL GUIDELINES AND PROCEDURES

Section 1.	AIDS Guidelines	2
Section 2.	System Office and Campus Closures (<i>formerly CM 05-01</i>)	3
Section 3.	Requests for Information and Open Communication (<i>formerly CM 99-01</i>)	3
Section 4.	Limit on Teaching for Graduate Teaching Assistants	4
Section 5.	Moving Expenses for Presidents (<i>formerly CM 95-2</i>)	4
Section 6.	No Smoking Law (<i>formerly CM 95-3</i>)	5
Section 7.	Council of Professional Police Standards (<i>formerly CM 03-02</i>)	6
Section 8.	System Expectations for Inter-Institutional Relationships (<i>formerly CM 96-01</i>)	10
Section 9.	Interim Information Security Plan for NSHE (<i>formerly CM 03-03</i>)	11
Section 10.	HIPAA Guidelines	14
Section 11.	HIPAA Health Care Components of NSHE	16
Section 12.	Campus Sex Crimes Prevention Act Compliance (<i>formerly CM 02-05</i>)	18
Section 13.	Internal Procedures for Telephone Charges	23
Section 14.	Annual and Sick Leave Record Keeping Guidelines	23
Section 15.	Phase-in Retirement Program	24
Section 16.	Conference/Training Policy	25

**NEVADA SYSTEM OF HIGHER EDUCATION
PROCEDURES AND GUIDELINES MANUAL**

CHAPTER 4

GENERAL GUIDELINES AND PROCEDURES

Section 1. AIDS Guidelines

1. The Nevada System of Higher Education, in order to address the personal, administrative, medical, and legal problems associated with the Acquired Immune Deficiency Syndrome (*AIDS*), has established the following guidelines. These are intended to provide direction for our institutions when dealing with the disease of AIDS and AIDS-related issues.
2. The primary response of Nevada System of Higher Education institutions to AIDS should be increasing awareness and education - for students, employees, faculty, and others. Effective education based upon the best currently available information will aid in preventing the spread of the disease.
3. Individuals will not be required to undergo screening for AIDS as a condition of enrollment, employment, or financial services. Faculty, students, and staff who are diagnosed as having AIDS, AIDS-related complex, or a positive antibody test and who are otherwise qualified should be afforded normal classroom attendance, working conditions, student housing, benefits, and participation in curricular and extracurricular activities in an unrestricted manner, as long as they are physically and psychologically able to do so. Decisions regarding such individuals will be made on a case-by-case basis, taking into account the individual's behavior and physical condition.
4. The American College Health Association prepares guidelines on aids related issues. It is suggested NSHE institutions refer to this report for guidance in addressing local needs.
5. It is also recommended that the Center for Disease Control guidelines be used to insure safety of students, staff, and faculty handling human blood, blood products, and other body secretions.
6. Each NSHE institution will establish procedures to respond to AIDS-related concerns, as well as to public inquiries.
7. The institution guidelines will be revised as necessary, in response to the release of new scientific information.

(B/R 6/88; Added 6/05)

Section 2. System Office and Campus Closures (formerly CM 05-01)

This is intended to clarify procedures for system and campus closures for any adverse event including weather.

1. The Chancellor (*or designee*) has sole authority to close the entire NSHE or any part of the system for unforeseen events *which may include but are not limited to* extreme weather conditions, natural disasters, or other emergencies. In the event the governor closes all or any part of the state offices, the Chancellor will be notified and will similarly declare NSHE properties closed, as appropriate. When the NSHE or any part of the system is closed, employees at the affected location(s) are granted administrative leave. No other person has authority to close offices or grant administrative leave.
2. The President (*or designee*) of each campus has the authority to close the campus for unforeseen events (as defined above). The President (*or designee*) must report such closure to the Chancellor and receive acknowledgement, *if possible*, prior to the closure, unless there is an emergency status that requires immediate action. In the event of a campus closure, employees at the affected institution or location will be granted administrative leave. No other person has the authority to close offices or grant administrative leave.
3. When campuses or offices are open, employees desiring not to report to work due to extreme weather conditions or natural disasters must request and receive approval of annual leave.
4. Employees on *previously approved* leave during a closure do not get administrative leave credit.

(Added 6/05)

Section 3. Requests for Information and Open Communication (formerly CM 99-01)

Requests for information come from many different sources from within the NSHE and externally. In order to provide guidance for NSHE units in answering or initiating these requests the following guidelines are advanced.

1. All requests should attempt to be answered in a timely manner.
2. If the request presents a burden of excessive time, resources or disruption of other priorities, all individuals should seek confirmation with their supervisor, referred up the line, before proceeding.
3. If a request cannot be honored, the decision maker should contact the requester and explain why. Complaints or questions should be referred up the line.
4. Regent's requests for information including document inspection or copying and preparation of reports are governed by Title 4, Chapter 1 of the Handbook. Requests must go to the Chancellor, Assistant Chancellor, Vice Chancellors, Presidents, Vice Presidents, Chief Administrative Officer or Director of Internal Audit, as the case may be. Each request must be copied to the Chancellor or President, as applicable.

5. Responses to information requests should be disseminated widely. All communication to members of a governance group should be sent simultaneously to all members of the group. This includes sending responses to all Regents when one Regent requests information (*see Title 4, Chapter 1 for details*).
6. Many governance groups have list serves that can be used for broad distribution. All matters that deal with a campus or campuses should be shared with the Presidents. Issues relating to faculty concerns, teaching, research and academic programs should be shared with Presidents and faculty senate chairs and the relevant system committees (*Academic Affairs committee, Human Resources Advisory committee and Research Affairs committee*). Issues relating to student government and student activities should be shared with Presidents and student government presidents as well as with the Student Affairs Committee.
7. It is recognized that some information must remain confidential but the overall intent of these guidelines are to provide open communication among all units of the NSHE.

(Added 6/05)

Section 4. Limit on Teaching for Graduate Teaching Assistants

Pursuant to Board policy, Title 4, Chapter 5, graduate teaching assistants may teach no more than two courses per semester subject to the following guidelines:

1. First year graduate assistants without prior teaching experience are to be assigned tasks to assist a professor; that is, grading papers, proctoring examinations, serving as laboratory assistants, leading discussion groups of a subdivided class.
2. First year graduate assistants will be expected to complete, during their first year, a special teaching methods course if they are to teach during their second year. First year graduate assistants may also teach under the supervision of a professor or director while concurrently taking a teaching methods course.
3. Second and third year graduate assistants, after evaluation by their departments, are to be allowed to teach courses following the prescribed course syllabus, in conformity with standards adopted by the department, and at a level determined by the department as appropriate for each individual.

(B/R 3/71, 6/85, 8/86; Added 6/05)

Section 5. Moving Expenses for Presidents (*formerly CM 95-2*)

New permanent appointees to the position of President of a NSHE institution may be reimbursed from institutional funds for the following expenses:

- ✓ Relocation travel: For the employee and immediate dependent family members.
- ✓ Moving household goods: Reasonable moving expenses for household goods that conform to State of Nevada guidelines and limits. Approval for moving expenses must be obtained from the Chancellor prior to incurring any such expense.

- ✓ Office and Professional Materials: Where such materials are deemed essential to the successful performance of the president as an administrator and/or as an academic faculty member, it is appropriate to be reimbursed for reasonable relocation expenses for office and professional material. Non-state appropriated funds must be used for this item. The extent and composition of allowable materials is subject to the approval of the Chancellor.

In the event that moving expenses exceed State of Nevada guidelines, such excess will be submitted to the Chancellor for review and approval at the Chancellor's discretion. Non-state appropriated funds must be used for any excess.

Should appointee leave employment voluntarily within the first twelve months, these moving and relocation expenses shall be repaid in full.
(Added 6/05)

Section 6. No Smoking Law (formerly CM 95-3)

Policy and State Law

Nevada Revised Statute 202.2491 prohibits the smoking of tobacco in any public building, except within a separate room or area of the building. The person in control of a public building is required to designate a separate room or area in which smoking is permitted and is further required to post "no smoking" signs in the building.

NSHE Vice Chancellor for Legal Affairs interprets this statute as permitting a person in control of a public building to designate only one room or area in a public building for smoking. The term "building" means any building owned by the Nevada System of Higher Education. It would obviously be inappropriate for any System employee to experience any employment retaliation for complaining about smoking in prohibited areas or for taking action to enforce the state law.

Penalties:

Nevada Revised Statute 202.2492 provides that any person who violates NRS 202.249 is guilty of a misdemeanor.

The posting of "no smoking" signs and the designation of a separate room or area in a public building for smoking, done pursuant to this law, constitute an order to employees not to smoke tobacco in a public building except in such a designated room or area. Violation of such an order would constitute insubordination, which conduct would authorize disciplinary action to be taken against classified employees under Nevada Administrative Code § 284.650 (6) and against professional employees under Section 6.2.1 (d) of the NSHE Code. Section 6.2.2 (m) of the NSHE Code also authorizes disciplinary action against professional employees who violate state law on System premises.

Implementation:

Please take the necessary steps to implement and inform your employees about this policy.
(Added 6/05)

Section 7. Council of Professional Police Standards
(formerly CM 03-02)

The Nevada System of Higher Education (*hereinafter "NSHE"*) requires NSHE institutions that have a police department to establish a system to review allegations of misconduct made against police department officers and employees. At present, the University of Nevada, Reno, the University of Nevada, Las Vegas, College of Southern Nevada and Truckee Meadows Community College are the only NSHE institutions that have a police department. The guidelines for establishing an institutional Council of Professional Police Standards are outlined in this procedure.

I. Name of the Council

The name of the council established at the University of Nevada, Reno shall be the Police Services Board of Professional Standards (*hereinafter "board or council."*)

The name of the council established at UNLV shall be the Council of Professional Police Standards. (*hereinafter "board or council."*)

The name of the board established at TMCC shall be called the TMCC Police Department Professional Standards Board. (*hereinafter "board or council."*)

II. Council Charge

The council shall review any allegation of misconduct against any employee of a police department of the NSHE and may make recommendations concerning actions of the department or an individual. An allegation of misconduct is defined as any allegation that may result in the imposition of criminal charges, demotion, suspension without pay, or termination. The council shall review investigative materials provided by the Director of Police Services of the University of Nevada, Reno, the Director of Public Safety of the University of Nevada, Las Vegas, or the Police Chief of the Truckee Meadows Community College Police Department (*hereinafter "department head."*)

The chair of the council shall issue a written report regarding the outcome of an investigation and of all complaints received, to the department head and to the President of the institution.

The department shall maintain a log of each complaint received which shall be assigned a chronological tracking number. Upon receipt, an investigation shall be conducted by the department head and those requiring review will be forwarded to the council. Any complaint lodged against the department head will be referred to the respective Vice president for investigation.

The council will convene when notified by the department head at the conclusion of an investigation, or upon request of the President of the institution or any member of the council. The department head will provide the council with copies of the completed internal reports, complaint, and all other information pertaining to the complaint. Personally identifying information concerning employees will be redacted from the documents provided to the council. In the event that confidential information other than personally identifying information is withheld from the council by the department head, the department head will disclose the fact that information was withheld to the council and describe the nature of the information withheld.

If, during the course of a calendar year, there are no allegations of misconduct reported, the council will convene no later than the last day of the spring semester to review *all* complaints received by each respective department.

A report summarizing the complaints, any allegations of police misconduct, and other council activities and actions will be forwarded annually, together with any recommendations, to the department head and the President of each respective institution, and to the Chancellor of the NSHE.

III. Structure of the Council

A. Appointment of Members

1. Council members will be selected by the President from a list of nominations submitted by the appropriate Vice President.
2. Council members selected by the President, and prior to appointment, will be subjected to a police background check in order to determine their suitability to serve on the Council and receive information that may be law enforcement sensitive. Felony convictions will be cause for disqualification. All other arrests or convictions may be cause for disqualification. The final decision on suitability for service shall rest with the President upon recommendation of the department head.
3. Nominees will be solicited no later than April 15 of odd numbered years and additionally as needed.
4. Members shall not be current or former members of any law enforcement agency, with the exception of the department head, who will serve in an ex-officio, non-voting capacity.

IV. Membership-University of Nevada, Reno

1. The Director of Police Services will serve in an ex-officio, non-voting capacity.
2. One classified employee from two nominated by the Staff Employees Council.
3. The Associated Students of the University of Nevada, Reno (*ASUN*) President or his/her designee.
4. One non-police member from the Police Advisory Board, who is nominated by the Advisory Board.

5. One administrative faculty member who holds the title Director, Associate Vice President, Assistant Vice President, or Vice President, nominated by the President's Council.
6. One member of the academic faculty from two nominated by the Faculty Senate.

V. Membership-University of Nevada, Las Vegas

1. No fewer than five members of the UNLV Public Safety Advisory Board who are not in law enforcement shall sit as members of the Council. The Public Safety Advisory Board includes students, faculty, professional staff, classified staff, and at large community members.

VI. Membership-Truckee Meadows Community College

1. The Chief of Police shall serve in an ex-officio, non-voting capacity.
2. The Vice President for Finance & Administration shall serve in an ex-officio, non-voting capacity.
3. One classified employee (*from two nominated by the Staff Employees Council.*)
4. One student government member (*the President of ASTM or his/her designee.*)
5. One non-police member from the Police Advisory Board (*nominated by the Advisory Board.*)
6. One administrative faculty member (*must hold the title of: Director, Associate Dean, or Dean nominated by the President's Cabinet.*)
7. One member of the academic faculty (*from two nominated by the Faculty Senate.*)
8. One community representative appointed by the President.

VII. Membership-College of Southern Nevada

1. Chief of Police, (*ex-officio, non-voting*)
2. One classified employee (*from two nominated by the classified council*)
3. One Student government member (*president of ASCCSN or designee*)
4. One non-police community member appointed by the President
5. One administrative faculty member (*from two nominated by the cabinet usually Dean or above*)
6. One member of the academic faculty (*from two nominated by the faculty senate*)
7. Chief campus administrator for West Charleston Campus, Cheyenne Campus and Henderson Campus

VIII. Terms of Office

1. Non-student members will serve two-year terms; Student members will serve one-year terms.
2. Nominations will be solicited by April 15, with the terms in office to begin the day after spring commencement and ending on the day of spring commencement after the appropriate term has been served.
3. Solicitations for nominations to replace vacancies will be sought without delay.
4. Members who show lack of interest, or who fail to complete the training requirements, may be replaced at the request of the department head after discussions with the council. Such a recommendation shall be approved by the President.

IX. Organization of the Council

1. The council will select by vote of those present at the first meeting of each newly appointed council, a chair and a vice-chair.
2. The chair, or in his/her absence, the vice-chair, will convene the council at the request of the department head, President, or other council member, set the agenda, preside at meetings, and serve as spokesperson for the council.
3. A secretary, provided by the department head, will record and distribute meeting notes and maintain the council's files and records.
4. There shall be no provisions for proxy. A majority of voting members constitutes a quorum that is necessary for the council to take action and conduct business. A simple majority of those present shall be required to pass a motion.
5. In the event of a tie, a motion shall be tabled until such time as all five members are present to vote.

X. Duties of the Council

- A. To fulfill the charge as outlined in II above:
 1. Present written recommendations, with supporting narrative, to the department head and to the President.
 2. Prior to the end of each spring semester, issue a written report summarizing the complaints made against officers, including any allegations of police misconduct and other board activities and actions, along with any recommendations, to the department head and the President, and to the Chancellor.
 3. Maintain the files and records of the council pursuant to NRS 239.073 and make them available to each successive council.

XI. Training Requirements

1. Council members shall be required to attend training provided by the respective department. Training shall consist of at least the following:
 - a. A four (4) hour ride-a-long with a sworn patrol officer of the department.
 - b. Three (3) hours of departmental orientation, familiarization with department policies, procedures, general orders, organizational makeup and authorized equipment. In addition, board members will receive orientation regarding the provisions of Chapter 284 of NRS, the regulations adopted pursuant thereto and NRS 289.010 to 289.120, the applicable sections of NRS 396.3291, NRS 179a, Chapter 239, and Board of Regents policy.
 - c. One (1) hour of orientation with policies and procedures of the NSHE personnel manual and the terms and conditions of employment of members of the department.

XII. Effective Date and Amendments

Nominations for council members will be solicited and appointments made in order for each council to commence their initial terms of office on the day after Spring 2003 commencement.

Amendments to this document are recommended by the council through the respective department head and President to the Chancellor. Amendments are effective immediately after review by legal counsel and approval by the Chancellor. Changes to this document shall be reported to the Board of Regents and brought to the Board for discussion if the changes are substantive.

(Added 6/05; A 10/08))

Section 8. System Expectations for Inter-Institutional Relationships *(formerly CM 96-01)*

The ways in which the institutions within the NSHE interact with each other define, to a large degree, the collegial and collective character of the System. Establishment and maintenance of proper codes of behavior for the conduct of interinstitutional relationship are the responsibility of the Chancellor.

The following principles shall establish a foundation for the System expectations:

1. Institutional Comparisons

Public statements by responsible institutional officers and official publications or other media releases by an NSHE institution shall contain no invidious comparisons about any other institution within the NSHE.

2. Resolution of Perceived Inequities

Perceptions of inequity in funding or other treatment, whether by region of the State or by type of institution, shall be referred to the Chancellor for analysis, explication and, if necessary, resolution. Such allegations should be supported by appropriate data, documentation and argument.

3. Presidential Authority

Presidents are accountable to the Chancellor for the ways in which their institution and its executive officers conduct their proper business with the other members of the NSHE and with the System Administration.

(Added 6/05)

Section 9. Interim Information Security Plan for NSHE *(formerly CM 03-03)*

- I. BACKGROUND.** Graham-Leach-Bliley Financial Services Modernization Act of 1999 (*GLB*), 15 U.S. Code §6801, 16 CFR, Part 314, mandates that in addition to complying with the Privacy Rules of FERPA and HIPPA, financial institutions must take steps to safeguard the security of customers' financial information. The FTC, which regulates this area, takes the position that these safeguarding rules apply to institutions of higher education. It governs non-public, personally identifiable financial information, such as student loan application information and social security numbers. The FTC has determined that institutions must comply with the Safeguards Rule by May 23, 2003. This Chancellor's Memorandum is intended to serve as the NSHE's Interim Information Security Plan in compliance with the FTC's Safeguards Rule. The sources for this Information Security Plan were obtained from materials provided by the National Association of College and University Business Officers and the National Association of College and University Attorneys.
- II. SCOPE OF THE SECURITY PLAN:** This Plan applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form, which is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.
- III. ELEMENTS OF THE SECURITY PLAN:**
 - 1. Risk Identification and Assessment.** To identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information whether in electronic, paper or other form. The Security Program Officer will coordinate the establishment of procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including: (1)

Employee training and management; (2) Information systems and information processing and disposal; and (3) Detecting, preventing and responding to attacks.

2. **Designing and Implementing Safeguards.** The Program Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards.
3. **Overseeing Service Providers.** The Security Program Officer shall coordinate with those responsible for the third party service procurement activities among the affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access.
4. **Adjustments to Plan.** The Program Officer is responsible for evaluating and adjusting the Plan based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Plan.

IV. DESIGNATED SECURITY PROGRAM OFFICER. The President of each institution shall designate a Security Program Officer for the coordination and execution of the information security plan. This designation must be made by May 23, 2003. All correspondence and inquiries should be directed to the Security Program Officer.

V. RELEVANT RISK ASSESSMENT AREAS. The following have been identified as relevant areas to be considered when assessing the risks to customer information:

- ✓ Employee Management and Training
- ✓ Information Systems
- ✓ Managing System Failures
- ✓ Student Loans
- ✓ Student Card Office
- ✓ Admissions
- ✓ Registrar's Office
- ✓ Financial Aid Office
- ✓ Accounts Receivable Office
- ✓ Residence Life
- ✓ Student Health Center
- ✓ Continuing Education
- ✓ Business Centers
- ✓ System Computing Services

VI. SECURITY POLICY COORDINATION. The Security Program Officer will coordinate with the above offices to maintain the information security program. The Security Program Officer will provide guidance in complying with all privacy regulations. Each relevant area is responsible to secure customer information in accordance with all privacy guidelines. A written security policy that details the information security policies and processes will be maintained by each relevant area and will be made available to the Security Program Officer upon request. In addition, the information technology department and SCS will maintain and provide access to policies and procedures that protect against any anticipated threats to the

security or integrity of electronic customer information and that guard against the unauthorized access or use of such information.

VII. SERVICE PROVIDERS' CONTRACTS. Each of the institutions within NSHE will select appropriate service providers that are given access to customer nonpublic financial information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Contracts with service providers shall include the following provisions:

An explicit acknowledgment that the contract allows the contract partner access to confidential information;

A specific definition of the confidential information being provided;

A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;

A guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;

A guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;

A provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;

A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;

A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles NSHE to immediately terminate the contract without penalty;

A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and

A provision ensuring that the contract's protective requirements shall survive any termination agreement.

These standards shall apply to all existing and future contracts entered into with such third party service providers. While contracts entered into prior to May 23, 2003 may be grandfathered, the Security Program Officer, in cooperation with the General Counsel's Office, will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

VIII. REASSESSMENT OF INFORMATION SECURITY PLAN. This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the institution's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance shall be done by the Security Program Officer. Annual risk assessment will be done through the Security Program Officer. Evaluation of the risk of new or changed business arrangements will be done through the General Counsel's office.

(Added 6/05)

Section 10. HIPAA Guidelines

The purpose of this section is to outline the basics of HIPAA. It may be useful to information technology, accounting, payroll, human resources and auditing staff who are not regularly involved in handling health care records. For more detailed information, you may contact one of HIPAA Privacy Officers for UNR, UNLV or CSN, or the Vice Chancellor for Legal Affairs Office of the NSHE.

What is HIPAA?

The Health Insurance Portability and Accountability Act (*HIPAA*) was enacted by Congress on 21 August 1996 to combat waste, fraud and abuse, improve portability of health insurance coverage, and simplify health care administration. HIPAA is intended to promote efficient electronic transmission of health information, enhance patient rights, and provide standards to protect the privacy and security of health information. There are two primary rules at issue. The Privacy Rule protects individually identifiable health information in all forms – verbal, written or electronic. The Security Rule concerns only individually identifiable health information that is maintained, transmitted or received in electronic form.

Who is covered?

The institutions within NSHE are not primarily health care providers. We are called a Hybrid Covered Entity under HIPAA, which means that we are allowed to designate which parts of NSHE are covered. Those entities and programs that are covered are free to share health care information with each other for legitimate purposes. Those entities or programs that are not covered may not receive or obtain access to identifiable health information unless authorized by the patient. As an example, most of the School of Medicine is covered; its Human Resources Department is not. It would not be appropriate for the School of Medicine to share a clinical record of an employee/patient with Human Resources unless the patient authorizes the disclosure. The Chancellor of NSHE has designated the covered programs and departments. This may be changed from time to time. Any program or department that is not covered is not required to follow any aspect of the Privacy or Security Rules.

Who must be covered?

Any program or department that provides a health related service and engages in certain electronic transactions related to payment must be covered. Those programs and departments that provide health related services, but do not engage in any of the specified electronic transactions may choose to be covered as it may assist them in interacting with patients and other providers in the health care industry. The specified electronic transactions include: health care claims, health care payment and remittance advice, coordination of benefits, health care claim status, enrollment and disenrollment in a health plan, eligibility for a health plan, health-plan premium payments, and referral certification and authorization.

Individually Identifiable Health Information

HIPAA protects only certain information that may identify a patient. This includes demographic information such as name, address, phone number, age over 70, dates of service and account numbers of all types (*social security, date of birth, drivers license, etc.*), as well as treatment and billing records.

Basic Privacy Rule Requirements

The Privacy Rule requires:

- Provide information to patients about their privacy rights and how their information can be used.
- Adoption of clear privacy procedures.
- Train employees so that they understand the privacy procedures.
- Designate an individual to be responsible for ensuring that the privacy procedures are adopted and followed.
- Secure patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Privacy Rule Limitations on Use

In general, treating professionals are allowed to freely exchange patient information as necessary for treatment without the necessity of obtaining patient authorization. In addition, a health care provider may use and submit information to obtain payment (*but not for insurance underwriting*), and for internal operations purposes (*such as a peer review committee*), without patient authorization. If outside non-treating vendors will require access to patient health information in order to perform a service for a covered program (*e.g. computer technician, copy service, record storage company, etc.*), patient authorization is required unless a business associate agreement is in place. Apart from certain disclosures that may be required in response to subpoenas and other law enforcement measures, any other disclosure outside the covered department requires written patient approval.

Privacy Rule Patient Rights

Patients are required to be informed of their rights under HIPAA, which include rights related to access to records, correction of records, and accounting for disclosures. There must be a mechanism in place to receive complaints. Civil and criminal penalties are in place for violations of the law. For example, improperly providing patient data for material gain could result in a criminal violation.

Security Rule Applicability

The Security Rule applies to all covered programs that receive, transmit or store health care records electronically.

Basic Security Rule Provisions

Administrative Procedures

Policies and procedures must be implemented and documented in each of these twelve areas:

- Training programs in security management and process issues
- Formal protocols for controlling access to data
- Internal audit procedures

- Contingency plan to ensure continuity and preservation of data in an emergency
- Security features for initial clearance of all personnel who have access to health information along with ongoing supervision, training and monitoring
- Security configuration management procedures such as virus checking, hardware and software systems review, and documentation
- Specific procedures when personnel terminate employment
- Security management structure that maintains continual risk assessment and sanction policies and procedures

Physical Safeguards

Data and data systems must be physically protected from intrusion and environmental hazards:

- Designation of a specific person for responsibility of security
- Controlling access to and altering of computer hardware
- Implementation of work station security activities
- Development of disaster/intrusion response and recovery plans
- Maintenance of security records
- Implementation of identity verification procedures to physically access sites

Technical Security Services

Software control and procedures regarding stored data include these requirements:

- Providing for internal audits and controls within data systems
- Control access by users through authentication
- Ensure that stored data is neither altered nor inappropriately accessed/processed
- Allow data access during crises

Technical Security Mechanisms

These requirements relate to accessed data and the transmission of stored data, to ensure that data cannot easily be accessed, intercepted or interpreted by unauthorized third parties.
(Added 6/05)

Section 11. HIPAA Health Care Components of NSHE

As of May 6, 2004, NSHE, a hybrid covered entity, designates its health care components as follows:

UNLV

- Dental School and any associated clinics
- Student Health Center & Pharmacy
- Student Wellness
- Athletic Training Department
- Center for Individual & Family Counseling
- Center for Health Information Analysis
- National Supercomputing Center for Energy and the Environment

UNR

- University of Nevada School of Medicine as a hybrid covered entity, and as an Organized Health
- Care Arrangement with its affiliated practice clinics MedSchool Associates South, MedSchool
- Associates North, and NFPRP (*Mojave Health*), but excluding from its designation the following
- Programs/Departments: Department of Geriatric Education, Southern Nevada AHEC, Facilities
- Management and Human Resources, Craniofacial Clinic, Sexual Abuse Medical Evaluation
- Clinic, and Medical Students Free Standing Clinic.
- Psychological Service Center
- Counseling and Testing
- CEP-Downing Clinic
- Athletic Training Department
- Student Health Center
- Pharmacy

CSN

- Dental Hygiene Clinic
- Dental Faculty Practice
- Diagnostic Medical Sonography

NSC, DRI, GBC, TMCC, WNC

- No departments or programs are included.

NSHE

- NSHE Accounting and Auditing
- NSHE General Counsel's Office,
- UNLV, UNR, and CSN Disbursement Offices
- NSHE, UNLV, UNR, and CSN health and insurance plans
- NSHE, UNLV, UNR, and CSN Information Technology Departments

(Added 6/05)

Section 12. Campus Sex Crimes Prevention Act Compliance *(formerly CM 02-05)*

A. THE FEDERAL CAMPUS SEX CRIMES PREVENTION ACT.

- 1. The Campus Sex Crimes Prevention Act (CSCPA) requires campuses to notify campus communities where law enforcement agency information concerning registered sex offenders may be obtained.**

The CSCPA requires sex offenders to register pursuant to State law and to provide notice of each institution of higher education at which the person is employed, carries on a vocation, or is a student and of each change in enrollment or employment status of such person at an institution of higher education in the State. The State must ensure that the registration information collected about offenders employed at or enrolled in institutions of higher education is promptly made available to a law enforcement agency having jurisdiction where such institution is located.¹

The institution is required to provide as a part of its annual security report:

A statement advising the campus community where law enforcement agency information provided by a State under section 170101(j) of the Violent Crime Control and Law Enforcement Act of 1994 (42 U.S.C. 14071(j)), concerning registered sex offenders may be obtained, such as the law enforcement agency with jurisdiction for the campus, or a computer network address.

20 U.S.C. § 1092(f)(1)(l).

- 2. The Proposed Guidelines for the Campus Sex Crimes Prevention Act (CSCPA) suggest that the Department of Justice will construe the CSCPA as imposing a duty on campus police departments to protect campus communities by providing community notification.**

The Department of Justice published proposed guidelines for the CSCPA on March 8, 2002. The proposed guidelines provide in part:

Subsection (j)'s requirement to promptly make the information available to a law enforcement agency having jurisdiction where the institution is located is supplementary to the requirement under subsection (b)(2)(A) and (4) of the Wetterling Act (42 U.S.C. 14071(b)(2)(A), (4)) to promptly make information concerning registrants available to a law enforcement agency having jurisdiction where the registrant resides. The legislative history of the Campus Sex Crimes Prevention Act explains subsection (j)'s requirement as follows:

¹ For NSHE institutions that do not have a campus police department, the "law enforcement agency having jurisdiction where such institution is located" is the law enforcement agency or agencies providing police protection to the institution. For institutions that do maintain a campus police department, several law enforcement agencies will have, as a legal proposition, concurrent jurisdiction where the institution is located, including the campus police department, the sheriff's office of a county, a police department of an incorporated city or a metropolitan police department. Despite the concurrent jurisdiction of multiple law enforcement agencies to provide police services to an institution, however, the campus police department may have primary responsibility for providing police protection to the institution pursuant to an Interlocal Agreement among the various police agencies.

Once information about an offender's enrollment at, or employment by, an institution of higher education has been provided to a state's sex offender registration program, that information should be shared with that school's law enforcement unit as soon as possible.

The reason for this is simple. An institution's law enforcement unit will have the most direct responsibility for protecting that school's community and daily contact with those that should be informed about the presence of the convicted offender.

If an institution does not have a campus police department, or other form of state recognized law enforcement agency, the sex offender information could then be shared with a local law enforcement agency having primary jurisdiction for the campus.

146 Cong. Rec. S102216 (Oct. 11, 2000) (remarks of Senator Kyl).

Thus, if an institution of higher education has a campus police department or other form of state recognized law enforcement agency, state procedures must ensure that information concerning the enrollment or employment of registrants at that institution (and subsequent changes in registrants' enrollment or employment status) is promptly made available to the campus police department or law enforcement agency. If there is no such department or agency at the institution, then state procedures must ensure that this information is promptly made available to some other law enforcement agency having jurisdiction where the institution is located. Regardless of whether an institution of higher education has its own law enforcement unit, the Wetterling Act does not limit the discretion of states to make the information concerning registrants enrolled or working at the institution available to other law enforcement agencies as well.

The CSCPA and the guidelines implementing the CSCPA require or expect that college and university police departments will provide the campus community with clear guidance as to where information about registered sex offenders can be found. Congress left to the colleges the discretion as to how to go about informing the campus communities of registered sex offenders in their midst. The overriding concern of the legislation is that campus police departments or law enforcement agencies responsible for providing police protection to campuses adequately protect the campus communities from registered sex offenders. In order to protect campus communities, campus police departments may have to provide greater notification to campus communities of the enrollment or employment of registered sex offenders than the CSCPA actually requires.

B. NEVADA'S SEX OFFENDER REGISTRATION LAW.

- 1. Nevada's sex offender registration law requires "the law enforcement agency in whose jurisdiction the sex offender resides or is a student or worker" to register sex offenders and provide community notification.**

NRS Chapter 179D, which is Nevada's sex offender registration law, requires "the law enforcement agency in whose jurisdiction the sex offender resides or is a student or worker" to register sex offenders and provide community notification of sex offenders within its territorial jurisdiction. NRS 179D.730. Sex offenders present within a jurisdiction for 48 hours or more also must register in the jurisdiction. NRS 179D.240, 179D.460.

NRS 179D.730 establishes minimum levels of community notification on the basis of an offender's risk of recidivism. If the risk of recidivism is low, the sex offender is assigned a Tier 1 level of notification. If the risk is moderate, the sex offender must be assigned a Tier 2 level of notification. If the risk of recidivism is high, the sex offender must be assigned a Tier 3 level of notification. NRS 179D.730 imposes a duty on "the law enforcement agency in whose jurisdiction the sex offender resides or is a student or worker" to provide the appropriate level of community notification.

"Local law enforcement agency" is defined in NRS 179D.050 to mean: "1. The sheriff's office of a county; 2. A metropolitan police department; or 3. A police department of an incorporated city." Although a campus police department has primary jurisdiction for providing police services to the campus community and would be "the law enforcement agency in whose jurisdiction the sex offender resides or is a student or worker" with respect to offenders enrolled at or employed by the college or university, it is not a "local law enforcement agency" responsible for providing community notification pursuant to State law because it is not listed in the definition of "local law enforcement agency" in NRS 179D.050.2

NRS Chapter 179D does not require college or university police departments to register sex offenders or to provide community notification of sex offenders who are enrolled in or employed by an institution or who are present for 48 hours or more because college and university police department departments are not included in the definition of "local law enforcement agency" in NRS 179D.050.

C. THE RESPONSIBILITIES OF NSHE INSTITUTIONS MAINTAINING CAMPUS POLICE DEPARTMENTS.

- 1. Because UNR, UNLV, AND TMCC police departments have assumed primary responsibility for providing police protection to their campuses in Interlocal Agreements with local law enforcement agencies, they are "the law enforcement agency" in whose jurisdiction the sex offender is a student or worker with a duty to register sex offenders and provide community notification pursuant to NRS chapter 179D.**

Although several law enforcement agencies have concurrent jurisdiction over UNR, UNLV, and TMCC's property, the agencies have, by agreement, made campus police departments primarily responsible for providing police protection to these campuses. Because these campus police departments have assumed the primary responsibility to provide police protection, these police departments are the "law enforcement agency in whose jurisdiction the sex offender is a student or worker" or in which the sex offender is present for 48 hours or more. These departments, accordingly, must register sex offenders and provide community notification to the campus communities pursuant to NRS Chapter 179D.3

² If the Nevada Legislature were to amend NRS 179D.050 by adding "college or university police departments" to the definition of "local law enforcement agency," then all of NRS Chapter 179D would apply to NSHE institutions maintaining campus police departments, and they would be required to register sex offenders and provide appropriate community notification.

³ "Worker" is defined broadly in NRS 179D.120:

A NSHE institution maintaining a campus police department must provide community notification consistent with the requirements of NRS 179D.730. When an offender is assigned a Tier 1 level of notification, meaning that the risk of recidivism is low, a campus police department will notify other law enforcement agencies that are likely to encounter the sex offender. This is required by the NRS 179D.730(1)(a). The offender's name may be posted to the campus police department's website. The campus police department may post the offender's picture and a description of the crime on the website, and may conduct community notification if the campus police department determines there may be a danger to the campus community. This is consistent with NRS 179D.710(3).

When an offender is assigned a Tier 2 level of notification, meaning the offender is a moderate risk of re-offending, the campus police department will notify other law enforcement agencies that are likely to encounter the sex offender and will notify schools, religious and youth organizations situated on or adjacent to the campus that are likely to encounter the sex offender. This level of notification is required by NRS 179D.730(1)(b). Where the campus police department determines that there may be a danger to the campus, the offender's name may be posted to the website, the offender's picture and a description of the crime may be posted on the website, and the campus police department may provide notification to the University community. These actions are consistent with NRS 179D.710(3).

When an offender is assigned a Tier 3 level of notification, meaning the offender is a high risk of re-offending, the campus police department will, in addition to providing the required Tier 1 and 2 level of notification, notify the campus community through the use of flyers, photographs, email, and other means designed to reach members of the campus community who are likely to encounter the sex offender. This level of notification is required by NRS 179D.730(1)(c).

When an offender is assigned a Tier 2 or 3 level of notification and the sex offender has committed a sexual offense against a person less than 18 years of age, the campus police department will provide the appropriate notification for Tier 2 or Tier 3 and, in addition, will notify: (a) motion picture theaters, other than adult motion picture theaters, which are likely to encounter the sex offender; and (b) businesses which are likely to encounter the sex offender and which primarily have children as customers or conduct events that primarily children attend. This level of notification must include a copy of a photograph of the sex offender and is required by NRS 179D.730(2).

1. "Worker" means a person who engages in or who knows or reasonably should know that he will engage in any type of occupation, employment, work or volunteer service on a full-time or part-time basis within this state for:

(a) Any period exceeding 14 days; or
(b) More than 30 days, in the aggregate, during any calendar year, whether or not the person engages in or will engage in the occupation, employment, work or volunteer service for compensation or for the purposes of a governmental or educational benefit.

2. The term includes, but is not limited to:

(a) A person who is self-employed.
(b) An employee of an independent contractor.
(c) A paid or unpaid intern, extern, aide, assistant or volunteer.

Chapter 179D sets forth minimum levels of notification and grants law enforcement the right to provide supplemental notification where the law enforcement agency determines the offender poses a threat to the safety of the public. The community notification procedures described in this procedure reflect what is required or permitted by law.

D. THE RESPONSIBILITIES OF NSHE INSTITUTIONS THAT DO NOT MAINTAIN CAMPUS POLICE DEPARTMENTS.

All NSHE institutions, including those that do not maintain campus police departments, must comply with the CSCPA by providing, as a part of its annual security report, “a statement advising the campus community where law enforcement agency information provided by a State . . . concerning registered sex offenders may be obtained, such as the law enforcement agency with jurisdiction for the campus, or a computer network address.”

NSHE institutions that do not maintain campus police departments should determine whether they are parties to Interlocal Agreements with local law enforcement agencies for the provisions of police protection to the campuses. Unless the colleges, by agreement, assumed responsibility for providing some level of police protection to their campuses that would trigger duties under Chapter 179D, the local law enforcement agency with jurisdiction for the campus would be responsible for registration and notification. The colleges also should communicate with the local law enforcement agencies with jurisdiction over the campus for the purpose of assuring themselves that information concerning registered sex offenders will be available to the campus community. If the colleges have assumed any responsibility for providing notification to the campus community, they must provide the minimum levels of notification required by NRS 179D.730.

E. LIABILITY.

An institution may be liable for the failure of its campus police department to disclose the enrollment or employment of a registered sex offender who assaults a student or employee. Although the CSCPA, which is part of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, provides that the failure to comply with the act does not create a cause of action against any institution of higher education or any employee of such an institution, a claim could be brought under State law alleging that the campus police department was negligent in failing to disclose or failing to adequately disclose the enrollment or employment of an offender. Similarly, institutions that do not maintain campus police departments, but which may have assumed responsibility for providing some degree of notification to the campus community, may be liable for failing to provide the notification required by NRS 179D.730.

Like the CSCPA, Chapter 179D contains an immunity provision shielding law enforcement agencies and its officers from liability for acts or omissions relating to the disclosure of information. However, campus police departments may not be able to make use of this immunity provision because campus police departments, which will register offenders and provide community notification pursuant to Interlocal Agreements, are not included in the definition of “local law enforcement agency” in NRS 179D.050.

Amendment of NRS 179D.050 would clarify the responsibility of campus police departments and would limit the liability of institutions by giving campus police departments the benefit of NRS 179D.850, which grants immunity for acts or omissions relating to the accuracy of information in a record of registration and the disclosure of or the failure to disclose information.

Questions about compliance with the Campus Sex Crimes Prevention Act or Chapter 179D should be addressed to the Vice Chancellor for Legal Affairs.
(Added 6/05)

Section 13. Internal Procedures for Telephone Charges

Sound internal control procedures require that each department be responsible for reviewing its telephone charges on a monthly basis. All telephone charges must be reviewed by a supervisor and initialed and dated, indicating review of such charges. The telephone charges should be filed at the department level for at least three years. Charging personal toll calls and personal cellular calls to institutional funds is strictly prohibited. All personal calls must be reimbursed to the institution by check made payable to Board of Regents.

Where assigned, access codes or pin numbers should not be shared. These codes should always be cancelled when an employee terminates his/her employment.
(Added 6/05; A. 11/05)

Section 14. Annual and Sick Leave Record Keeping Guidelines

Per Title 4, Chapter 3 of the Board of Regents Handbook each appointing authority must keep accurate and complete records of earned and used leave for each NSHE employee. Such records will be kept as designated by the appropriate Human Resource office. Leave records are subject to examination by those persons in the employee's chain of command, by Human Resource officials, and by internal or external auditors.

Insofar as possible, all leave must be requested and approved in advance by the supervisor or other appropriate administrative officer according to the policies for each type of leave as contained chapter 3 of the Handbook. The approval and recording of unanticipated leave must occur immediately after use of the leave.

Sick Leave: Full-time professional staff members on an "A" or "B" contract shall be granted sick leave as required, up to 30 working days at full salary, available at any time during the initial 12 months of service. Part-time professional staff members on an "A" or "B" contract shall be granted a pro rata amount as appropriate.

Beginning one year after the starting date of his or her initial contract, each full-time staff member will begin to accrue additional sick leave at the rate of two days for each full month of paid service, to be added to any remaining balance of unused sick leave from the first 12 months of service. Sick Leave may be cumulative from year to year, not to exceed 96 days as of the first day of each fiscal year, and any sick leave in excess of 96 days is forfeited on that date. Part-time staff members will earn a pro rata amount of sick leave for each calendar month worked.

Paid sick leave shall not be granted in excess of sick leave earned except as provided in the extended salary sick leave policy as outlined in Title 4, Chapter 3. The employee shall not be paid for any unused sick leave upon termination of employment.

Annual Leave: All professional staff members on a full-time 12-month appointment ("A" contract) earn annual leave at the rate of two working days for each full calendar month of service. Prorated credit shall be earned for partial months of service. Professional staff members on a part-time 12-month appointment earn pro rata annual leave credit.

Annual leave may be cumulative from year to year, not to exceed 48 days as of the first day of each fiscal year, and any annual leave in excess of 48 days is forfeited on that date. No compensation will be authorized for unused or excess leave at the end of each fiscal year. Earned annual leave shall be taken at a time approved or directed by the supervisor or other appropriate administrative officer. Insofar as possible, approval to use annual leave must be secured in advance, in accordance with the provisions contained in Title 4, Chapter 3.

Employees shall be given an opportunity to use accumulated annual leave in excess of 48 working days prior to the last day of the fiscal year provided a request for leave is given by the employee no later than April 1 to the supervisor or other appropriate administrative officer.

Professional staff on an "A" contract appointment who resign or retire shall be entitled to be paid for unused accumulated annual leave up to the maximum of 48 days, unless the supervisor or other appropriate administrative officer directs the employee, in writing, to use all or a portion of the accumulated leave prior to the final date of employment.
(Added 6/05; A. 12/05)

Section 15. Phase-in Retirement Program

This program allows faculty and professional staff to phase-in their retirement (generally between a .50 and .75 FTE course load or work assignment) over an agreed-upon period of time, not to exceed 5 years. During the phase-in, the institution and employee will continue contributing to their retirement plan as if they were employed 100% FTE.

The phase-in process is governed by a formal contract between the employee and the NSHE. The basic provisions of the program are outlined below. If you have further questions about the phased-in retirement program, please contact the Human Resources Office on your campus.

Eligibility

The employee must have attained the age of 65 and completed at least 5 years of service with the institution at the expiration of the term of the agreement;

OR

have attained the age of 60 and completed at least 10 years of service with the institution at the expiration of the term of the agreement;

OR

at any age have completed 30 or more years of service with the institution at the expiration of the term of the agreement.

Process

- The employee requests an application form from the institution's Human Resource office.
- The employee completes the application and forwards it through the chain of command for signatures from the employee's chairperson, dean, provost/vice president, and president.
- The completed and signed form is sent to the campus Human Resources office, which officially determines eligibility.
- Human Resources notifies the employee of the status of their application.
- If the application is approved, the Human Resources office types the formal agreement and sends the agreement through the chain of command for signatures.
- No contract exists until such time as the agreement has been fully executed by the president of the institution.
- Any changes to the agreement, once executed, must be endorsed by the president and approved by the NSHE chancellor.

Enrollment Period and Application Deadline

- Completed applications for consideration of phased-in retirement for application forms will be due on February 1 of each year for the following fall semester. The form must contain all required signatures by that date.

(Added 6/05; A. 12/05)

Section 16. Conference/Training Policy

All System professional staff are eligible to request attendance annually for one out of state conference/meeting, to be paid for by the System that is applicable to their job duties and is approved by their supervisor. Any exceptions to this policy must be approved by the Chancellor.

(Added 7/06)