

ICU PRIVILEGES

____ I do not wish to have ICU privileges at Los Alamos Medical Center.

These privileges may be requested by physicians seeking privileges in Adult Medicine or in General Surgery as appropriate. Application for these privileges is evaluated on an individual basis and is subject to the approval of the Credentials and Executive Committees. Proof of competency may be required.

PROCEDURE	REQUESTED	REQUEST WITH SUPERVISION	RECOMMEND	RECOMMEND WITH SUPERVISION
Medical				
Complicated Myocardial				
Uncomplicated Myocardial				
Surgery				

Applicant's Signature

Date

Service Chief

Date

Credentials Committee

Date

Los Alamos Medical Center

Patient Restraint Physician Information

Physicians and other Licensed Independent Practitioners (LIPs) are required to have a “working knowledge” of Los Alamos Medical Center’s policy on restraint. Following are the most important points from the restraint policy:

Definitions

Physical Restraints - any manual method that immobilizes or reduces the ability of a patient to move his or her arms, legs, body, or head freely. Holding a patient in a manner that restricts his/her movement constitutes restraint for that patient.

Chemical Restraints - drug used as a restraint; a medicine used to control behavior or to restrict the patient’s freedom of movement and is not a standard treatment or dosage for the patient’s medical or psychiatric condition.

Restraint to Promote Medical Recovery (non-violent): refers to the use of restraints in those patients who require various medically essential therapies while hospitalized and who demonstrate a state of confusion or altered cognition that puts those therapies at risk OR those patients who require management of non-psychiatric behaviors that put them at risk for injury.

Restraints for Violent or Self-Destructive Behavior: refers to the use of restraints in those patients who require management of violent or self-destructive behavior towards themselves or others (including caregivers or other patients) or, who require physical restraint to manage suicidal or homicidal behaviors in ANY setting.

Restrictive Devices Applied by Law Enforcement Officials - handcuffs and other restrictive devices applied by law enforcement officials for custody, detention, and public safety reasons and not for the provision of health care are not considered restraints

Seclusion- seclusion is the involuntary confinement of a patient alone in a room or area from which the patient is physically prevented from leaving. Seclusion may only be used for the management of violent or self-destructive behavior that jeopardizes the immediate physical safety of the patient, a staff member, or others. **Seclusion is not used at Los Alamos Medical Center**

Use of restraint is assessment driven and is only implemented when:

Deemed necessary to protect the physical safety of patients, staff members or others AND less restrictive measures have been considered and/or attempted and found ineffective.

ORDERING

Medical Recovery Restraint: to protect the patient from self injury and to promote healing (prevention of dislodging of ET tube, lines, etc.) must be ordered by a LIP with a NEW order every calendar day based on the LIP's evaluation of the patient.

- ✓ A registered nurse may initiate restraints and obtain an order from an LIP who is responsible for the patient, as soon as possible after restraint is initiated
- ✓ The attending physician must be notified as soon as possible (can be through review of the restraint order) but no later than the end of the calendar day following initiation of the restraint order), if he/she was not LIP initiating restraint

Restraint for violent and/or self destructive behavior: jeopardizes the immediate safety of the patient, a staff member or others shall remain in effect until the patient's behavior or situation no longer requires the use of restraint, but no longer than

- ✓ 4 hours for adults 18 years of age or older;
- ✓ 2 hours for children and adolescents 9 to 17 years of age; or
- ✓ 1 hour for children 8 years of age or younger.

Renewal orders may be given for the above durations if the indications for restraint or seclusion persist. However, continuation of restraint or seclusion for longer than 24 hours shall be based on an in-person evaluation by a responsible licensed independent practitioner.

PRN orders for restraint are NOT to be used.

Face-to-Face Assessment performed within one-hour: A responsible licensed independent practitioner, a registered nurse or a physician's assistant shall perform a face-to-face assessment of the patient's physical and psychological status within 1 hour of the initiation of restraint.

Documentation of the LIP assessment for violent self destructive behavior restraint must include

- ✓ evaluation of the patient's immediate situation
- ✓ patient's reaction to the intervention
- ✓ patient's medical and behavioral condition
- ✓ need to continue or terminate restraint

The complete policy is available for your review in the Clinical Policy Manual on request. If any member of the medical staff has any questions regarding Los Alamos Medical Center's policy on restraint, please contact the Quality Department or Medical Staff Coordinator at hospital extension 1946, 1170.

I have read and understand the information on management of the patient in restraint at Los Alamos Medical Center.

Signature

Date

Printed name

HCA

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Information Confidentiality and Security Agreements
PAGE: 1 of 3	REPLACES POLICY DATED: August 15, 2001; Nov. 1, 2001; Jan. 27, 2004
EFFECTIVE DATE: April 30, 2005	REFERENCE NUMBER: IS.SEC.005

SCOPE: All Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, physician practices, home health agencies, service centers, and all Corporate Departments, Groups and Divisions.

PURPOSE: To provide awareness of the importance of information security and confidentiality and to authorize and require agreements with individuals and external entities to protect Company information resources, including confidential patient information.

POLICY:

A. Information Confidentiality and Security Agreements with Individuals.

1. All Company employees and other individuals granted access to Company information systems must sign and abide by the Confidentiality and Security Agreement (Agreement). The Agreement acknowledges specific responsibilities the individual has in relation to information security and the protection of sensitive information, including confidential patient information, from unauthorized disclosure.
2. A non-Company owned physician practice, vendor, or other external entity may make and shall enforce such Agreements on behalf of employees working off-site (*e.g.*, contracted transcription service, electronic claims submissions support contractor, physician office practice), if stipulated in the Company's contract with the external entity (see B. below). Each individual working on Company premises accessing Company and/or patient information must sign an Agreement.
3. The Information Security Steering Committee reviews and approves recommended changes to the Agreement, and Information Technology & Services (IT&S) publishes and maintains the Agreement. The Agreement is an official corporate document and must not be altered in any manner without prior approval from IT&S.

B. Contracts with Business Partners. Relationships with an external entity involving access to Company information systems or the exchange, transmission, or use of sensitive Company information require a formal contract including provisions to protect the confidentiality and security of the information and/or systems.

1. A Company representative authorized to approve access to the Company information system and/or the disclosure of the sensitive Company information must sign the Contract.
2. The Contract must include provisions governing the entity's information security policies and practices, as well as requirements to support Company compliance with

HCA

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Information Confidentiality and Security Agreements
PAGE: 2 of 3	REPLACES POLICY DATED: August 15, 2001; Nov. 1, 2001; Jan. 27, 2004
EFFECTIVE DATE: April 30, 2005	REFERENCE NUMBER: IS.SEC.005

regulatory requirements.

3. Current required Contract provisions are provided by the Legal Department.

C. **Contracts for IT&S Services.** All contracts for services will include appropriate standard security language approved by IT&S.

D. **Sanctions.** Violations of this policy could lead to disciplinary measures up to and including termination of employment or business relationship. Suspected violations of this policy are to be handled in accordance with the Information Security Policy, IS.SEC.001 and the Discipline section of the Code of Conduct. The Company encourages resolution at the local level and each Customer (an organization, business entity or organizational unit that has an established business relationship with IT&S as described in this policy's scope) will designate a process for reporting violations. In addition, violations may be reported to the Ethics Line at 1-800-455-1996.

E. **Policy Exceptions.** Exceptions to Security Policy are to be submitted to the IT&S Security Policy key contact for review and approval.

PROCEDURE:

A. The Confidentiality & Security Agreement form will be posted and maintained by IT&S on the Company Intranet located under Security.

B. Each Company employee must sign the Agreement at the time of employment and acknowledge the Agreement at the time of the Code of Conduct refresher training. The completed agreement will be maintained in the individual's personnel folder.

C. Each physician and allied health professional must sign the Agreement at the time he or she is appointed to a facility's medical staff and during the reappointment process thereafter. Completed Agreements will be maintained in the individual's credentials file.

D. Each volunteer must sign the agreement before beginning his or her service and annually thereafter. The agreement signature process and subsequent annual verifications can be completed during Code of Conduct training (if the volunteer attends such training), volunteer orientation or separately. The completed agreement will be maintained with the Company's records of the volunteer's service.

E. Physician office staff must sign the Agreement at the time information access is granted, and on an annual basis thereafter. Completed Agreements must be maintained in a central location by the Physician Support Coordinator or individual with a similar role in the business

HCA

DEPARTMENT: Information Technology & Services	POLICY DESCRIPTION: Information Confidentiality and Security Agreements
PAGE: 3 of 3	REPLACES POLICY DATED: August 15, 2001; Nov. 1, 2001; Jan. 27, 2004
EFFECTIVE DATE: April 30, 2005	REFERENCE NUMBER: IS.SEC.005

unit.

- F. Representatives of vendors and other external entities must sign the Agreement at the time information access is granted and at contract renewal or, at a minimum, every two years thereafter. Completed agreements must be maintained in the individual contract folder by the Facility CFO or designee.

REFERENCES:

Code of Conduct
Confidentiality & Security Agreement
Information Systems Security Policy, IS.SEC.001
Electronic Communications Policy, IS.SEC.002
CPCS Appropriate Access Toolkit

Confidentiality and Security Agreement

I understand that the facility or business entity (the “Company”) in which or for whom I work, volunteer or provide services, or with whom the entity (e.g., physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information (the “Company”), has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients’ health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, “Confidential Information”).

In the course of my employment / assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company’s Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

- | | |
|---|--|
| <ol style="list-style-type: none"> 1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. 2. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. 3. I will not discuss Confidential Information where others can overhear the conversation. It is not acceptable to discuss Confidential Information even if the patient’s name is not used. 4. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information. 5. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company. 6. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company. 7. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company. 8. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company. 9. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company’s policies. 10. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals. 11. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including e-mail, in order to manage systems and enforce security. 12. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and position screens away from public view. | <ol style="list-style-type: none"> 13. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards. 14. I will: <ol style="list-style-type: none"> a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)). b. Use only approved licensed software. c. Use a device with virus protection software. 15. I will never: <ol style="list-style-type: none"> a. Share/disclose user-IDs, passwords or tokens. b. Use tools or techniques to break/exploit security measures. c. Connect to unauthorized networks through the systems or devices. 16. I will notify my manager, Local Security Coordinator (LSC), or appropriate Information Services person if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information. <p>The following statements apply to physicians using Company systems containing patient identifiable health information (e.g. CPCS/Meditech):</p> <ol style="list-style-type: none"> 17. I will only access software systems to review patient records when I have that patient’s consent to do so. By accessing a patient’s record, I am affirmatively representing to the Company at the time of each access that I have the requisite patient consent to do so, and the Company may rely on that representation in granting such access to me. 18. I will insure that only appropriate personnel in my office will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access. 19. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information. |
|---|--|

Signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Employee/Consultant/Vendor/Office Staff/Physician Signature	Facility Name and COID	Date
Employee/Consultant/Vendor/Office Staff/Physician Printed Name	Business Entity Name	



Signature/Initial Page

This form will be placed in your medical staff file and in Medical Records for a signature and initial comparison on your charts. Please sign and initial where indicated.

Practitioner Printed Name

Practitioner Initials

Practitioner Signature

Applicant's Attestation

I, _____, certify that the information I have provided and the statements I have made on this application are correct, true, and complete to the best of my knowledge. I will abide by the applicable bylaws, rules and regulations, and policies and procedures of the designated health care entity. I acknowledge that I have received and reviewed a copy of the bylaws, if applicable, of the designated health care entity. I further agree that, in the event there should arise an adverse ruling with respect to my status and/or clinical privileges, I will exhaust the administrative remedies afforded by the entity's bylaws before resorting to litigation.

Signature stamps and date stamps are not acceptable.

Signature
type) _____
Date (do not

All applicants have the right to be informed of their application status. Application status inquiries should be directed to the appropriate health care organization. Practitioners may utilize any or all of the following to ensure accurate file information.

- **The right of practitioners to review information submitted to support their credentialing application.**
- **The right of practitioners to correct erroneous information.**
- **The right of practitioners to be informed of the status of their credentialing or recredentialing application upon request.**
- **The right of practitioners to be notified of these rights.**

This application has been designed to streamline the credentials verification process for providers, and meets the standards of many accrediting organizations. The application will be processed in accordance with the customer's required standards.

Hospital Services Corporation, a subsidiary of the New Mexico Hospitals and Health Systems Association, maintains this form, as well as a user's mailing list, to distribute any subsequent revisions. If you have any questions about this form or if you would like to be included on the user's list, please contact one of our credentials analysts at (505) 343-0070, or by e-mail at cvs@nmhsc.com. This application has been copyrighted and is intended for the sole use of our customers and approved users.

LOS ALAMOS MEDICAL CENTER

RELEASE OF INFORMATION

By signing this application, I hereby agree to cooperate fully with this institution, its medical staff, administrator, owner, operator and their agents, employees, attorneys and such other persons or entities as may be necessary or appropriate in the sole and exclusive discretion and judgment of the institution during its investigation and processing of this application. I further signify my willingness to appear for all interviews, submit documents, written or oral evidence or such other information as may be requested of me with regard to my application and I hereby expressly authorize the **Los Alamos Medical Center**, its medical staff, administrator, owner, operator and their agents, employees and attorneys to consult with and obtain oral or written information from such other persons or entities as they may deem appropriate who may have information or evidence bearing on my competence, background, education, experience, character, physical and mental condition and ethical qualifications. I further consent to this institution and its medical staff, administrator, owner, operator and their agents, employees and attorneys examining all records, documents and information that in their judgment and discretion may be material or relevant to an evaluation of this application and my professional qualifications and competence to perform the clinical privileges I have or may request as well as my moral, physical and ethical qualifications. I hereby release, acquit and forever discharge the above named institution, its medical staff, administrator, owner, operator and their agents, employees and attorneys and any and all other entities and persons who may furnish or submit documents, written or oral evidence or information in connection with the investigation and processing of this application from and of any liability, claim, cause of action or demand for or by reason of any matter, cause or thing in connections with the investigation and processing of this application, including, but not limited to, liability, causes of action or claims for invasion of privacy, libel, slander and negligence which may or could arise from the submission, giving, transmission, furnishing or discussion of documents, written or oral evidence or information touching on or related to my competence, education, background, character, experience, physical and mental condition and ethical qualifications.

Signature of Applicant

Date

Printed Name of Applicant

Dates: To / From _____

Job Title _____

Reason for Leaving _____

Education (use additional page if needed)

Institute Name

City, State

Dates Attended

Graduated? Yes No

Degree Earned

Institute Name

City, State

Dates Attended

Graduated? Yes No

Degree Earned

Please provide three (3) Professional References

1. _____
Reference Name

City, State

Phone Number

2. _____
Reference Name

City, State

Phone Number

3. _____
Reference Name

City, State

Phone Number

Have you ever been convicted of a crime? No Yes If yes, please provide city and state of conviction and details of conviction.

FAIR CREDIT REPORTING ACT NOTICE:

In accordance with the Fair Credit Reporting Act (FCRA, Public Law 91-508, Title VI), this information may only be used to verify a statement(s) made by an individual in connection with legitimate business needs. The depth of information available varies from state to state. Status of updates are available on request. Although every effort has been made to assure accuracy, General Information Services, Inc. cannot act as guarantor of information accuracy or completeness. Final verification of an individual's identity and proper use of report contents are the user's responsibility. General Information Services, Inc.'s policy requires purchasers of these reports to have signed a Service Agreement. This assures General Information Services, Inc. that users are familiar with and will abide by their obligations, as stated in the **FCRA**, to the individuals named in these reports. If information contained in this report is responsible for the suspension or termination of an employee or the application process, have the Candidate/employee contact General Information Services, Inc.

NOTICE TO CALIFORNIA CANDIDATES

You have a right to obtain a copy of any consumer report or investigative consumer report obtained by LIFEPOINT HOSPITALS, INC by checking the box provided below. The report will be provided to you within three (3) business days after we receive the requested reports related to the matter investigated.

I request to receive a free copy of this report by checking this box.

Under section 1786.22 of the California Civil Code, you may view the file maintained on you by GIS during normal business hours. You may also obtain a copy of this file upon submitting proper identification and paying the costs of duplication services, by appearing at GIS in person or by mail. You may also receive a summary of the file by telephone. The agency is required to have personnel available to explain your file to you and the agency must explain to you any coded information appearing in your file. If you appear in person, a person of your choice may accompany you, provided that this person furnishes proper identification.



By signing this page I acknowledge that I have received, read and have been given the opportunity to ask questions about the following documents:

"As an applicant for medical staff membership and clinical privileges I acknowledge that I have received a copy of the hospital's Medical Staff Bylaws, Rules and Regulations, Policies and Procedures, and Code of Conduct; and (i) if granted medical staff membership and clinical privileges, I agree to be bound by the terms of these documents, (ii) without regard to whether or not the application is granted, I agree to be bound by the terms thereof in all matters relating to consideration of the application and acknowledge the provisions in the bylaws for release and immunity from civil liability."

1. Medical Staff Bylaws
2. Medical Staff Rules and Regulations
3. Fair Hearing Plan

Practitioner Signature

Date Signed



ELECTRONIC SIGNATURE AUTHENTICATION STATEMENT

I, _____, hereby state that I
alone will have access to my signature key and will allow access to
nobody other than myself.

Name (Print)

Date

Name (signature)

Electronic Signature Statement