

MOUNT NITTANY HEALTH

CONFIDENTIALITY STATEMENT

I understand that in the performance of my duties or exercise of my privileges as an employee, volunteer, Medical Staff member, or other person authorized by Mount Nittany Health, or as an applicant for any such positions, I may have access to and may be involved in the processing of confidential patient care information and/or confidential personnel information (together "confidential information", see definitions on the other side of this form) whether in electronic form, paper form or through direct observation. I understand that I am required to maintain the confidentiality of such information received by me at all times, both at work and off duty, and that my duty of confidentiality includes the proper safeguarding and disposition of confidential information in a manner that prevents unauthorized access and disclosure.

I understand that access to and use of confidential information for legitimate purposes is a privilege and not a right, and that loss of that privilege may occur if I violate the terms of this statement, among other potential penalties. I acknowledge that a breach of confidentiality occurs if I obtain access to confidential information of any kind or in any manner that is not consistent with the requirements of my job or role with the Mount Nittany Health. I acknowledge further that a breach of confidentiality occurs if I disclose confidential information by any means to any person or entity not authorized to receive it. I understand that these rules against access and disclosure specifically include confidential information about me and my family members, friends and co-workers.

I understand that a breach of my duty of confidentiality may result in disciplinary action including termination of my employment or privileges. I further understand that a breach of my duty of confidentiality may result in legal action or criminal charges against me individually, and that the Mount Nittany Health will maintain this statement on file indefinitely. I certify by my signature that I have received education concerning my obligation and duty to protect the privacy of confidential information as defined herein and within the Mount Nittany Health policies.

I certify that I am the only person using and in possession of the confidential passwords for computer system access that may have been issued to me or specified by me. Misuse of passwords is a violation of my duty of confidentiality and I understand that any action taken using my passwords will be deemed an action taken by me. I understand that violations of professional standards for the protection of confidential information are violations of professional ethics and/or law and may be reportable to one or more of the following: the appropriate State Board of Licensure; the Secretary of Health and Human Services of the United States; and state or federal law enforcement officials.

I understand that the requirement of confidentiality and my personal liability for any breach of that confidentiality continue indefinitely whether or not I remain employed by or associated with the Mount Nittany Health or any of its affiliated entities.

Printed Name: _____

Signature: _____

Date: _____

- Employee**
- Physician**
- Contract Worker**

- Volunteer**
- Student**
- Other:** _____

MOUNT NITTANY HEALTH ADDENDUM TO CONFIDENTIALITY STATEMENT

Confidential patient information is defined as any information that is paper-based, electronic, orally transmitted or observed that includes the identity of the patient and any associated data pertaining to the health of the patient, tests or therapies provided to the patient, health insurance data or billing data, address or telephone number, social security number, or any subset of patient data that may be used to identify the patient to whom it applies.

Examples of **unauthorized access** to confidential patient information include, but are not limited to, the following: viewing patient identifiable information in any form and/or by any means that is outside the scope of job or role; participating in or listening to conversations about patients not under one's direct job responsibility or role; viewing patient schedules or similar documents when not part of the job or role; loitering in patient care areas without legitimate business reason; sharing or other misuse of passwords.

Examples of **unauthorized disclosure** of confidential patient information include, but are not limited to, the following: conducting a conversation about a patient when unauthorized persons are present and the conversation could take place in a secure area; intentionally or unintentionally leaving patient records or computer screens or systems accessible to unauthorized persons; permitting unauthorized persons to be in restricted areas such as unit stations or HIM where inadvertent disclosure is likely; directly disclosing patient information to any person not authorized to receive it by patient permission, job or role; disclosing to any unauthorized person that a patient was seen in the Medical Center receiving services, such as "Mom, I saw Betty in the Medical Center yesterday waiting to have a CT scan. Do you know what is wrong with her?"

Examples of **unauthorized disposition or disposal** of confidential patient information include, but are not limited to, the following: disposal of any patient records or patient identifiable information in the regular trash or recycling bins instead of the shredding box, including labels or notes identifying the patient; removing patient records or identifiable notes from the Medical Center when not authorized to do so; sending patient records via interdepartmental mail; misdirecting patient reports or other patient information to persons other than the authorized recipient.

Confidential personnel information is defined as records and information relating to payroll, salary, performance evaluations and related matters, disciplinary actions, attendance, employee health, disability, ADA matters, insurance benefit utilization, prescriptions, beneficiaries, dependents, court orders, wage attachments, employment applications, social security numbers, other contents of personnel files, contents of Medical Staff applications and files, and peer review information.

Examples of **unauthorized access to, disclosure of and disposition and disposal of** confidential personnel information are identical to or similar to the examples cited above for confidential patient information. Access is restricted to those persons authorized by job or role, and only for legitimate business purposes. Disclosure to unauthorized persons is prohibited except as may be provided for in Medical Center or Human Resources policy or provided by law. All such information must be kept secure from unauthorized access or disclosure, transported by hand or secure computer transaction rather than interdepartmental mail, and disposed of by shredding or transporting to Human Resources according to related Medical Center policies.