

ANESTHESIOLOGY INFORMATION TECHNOLOGY USER ID APPLICATION / UPDATE

RETURN INSTRUCTIONS: FAX TO 4-1798

SECTION I: TO BE COMPLETED BY EMPLOYEE

TYPE OF REQUEST: NEW CHANGE UPDATE DELETION TRANSFER

ACCOUNTS NEEDED: LAN ACCOUNT OUTLOOK

1. EMPLOYEE LAST NAME: _____

EMPLOYEE FIRST NAME: _____

2. LAST FOUR DIGITS SSN#: _____ DATE OF BIRTH: _____

3. BUILDING: _____ ROOM #: _____ PHONE #: _____

4. JHED ID: _____ INSTITUTION: JHH JHU

5. JOB TITLE/CLASSIFICATION: _____

6. EMPLOYMENT TYPE: STAFF FACULTY STUDENT TEMP

DATE TEMPORARY EMPLOYMENT ENDS: _____

7. SPECIAL NOTES: _____

8. SUPERVISOR SIGNATURE: _____ PHONE #: _____

9. EMPLOYEE SIGNATURE: _____ DATE: _____

Before sending this application please be sure that ALL items have been answered, or we will be unable to create your account. Please allow our staff at least 3 days to complete your request. Your Supervisor will notify you when your User ID is activated or in some cases we will be able to call you directly. If you have any questions regarding this form please call us at 5-2220.

SECTION II: TO BE COMPLETED BY ACCM IT

1. USER ID: _____ PASSWORD: _____

2. ACCOUNT: CREATED MODIFIED DELETED

3. ACTION COMPLETED BY: _____ DATE: _____

**CONFIDENTIALITY PLEDGE FOR ALL WORKFORCE
MEMBERS EXCEPT CONSULTANTS, CONTRACTORS AND VENDORS**

I understand that I require information to perform my duties at Johns Hopkins. This information may include, but is not limited to, information on patients, employees, students, other workforce members, donors, research, and financial and business operations. Some of this information is made confidential by law (such as “protected health information” or “PHI” under the federal Health Insurance Portability and Accountability Act) or by Johns Hopkins policies. Confidential information may be in any form, e.g., written, electronic, oral, overheard or observed. Access to all confidential information is granted on a need-to-know basis. A need-to-know is defined as information access that is required in order to perform my work or volunteer duties or to complete my approved academic requirements. If my duties change or my course of study changes, my need-to-know also may change.

I pledge to review the Johns Hopkins policies on confidentiality and privacy. I will access, use and disclose confidential information in keeping with these policies and only on a need-to-know basis. Before I make any other use or disclosure of confidential information, I will contact my supervisor or manager (if applicable) in order to obtain proper permission. If I have no manager or I am the manager, I will assure that the use or disclosure is within the law and Johns Hopkins policies.

I will not disclose confidential information to patients, friends, relatives, co-workers or anyone else except as permitted by Johns Hopkins policies and applicable law and as required to perform my work or volunteer duties or to complete my academic requirements.

I will protect the confidentiality of all confidential information, including PHI, while at Johns Hopkins and after I leave Johns Hopkins. All confidential information remains the property of Johns Hopkins and may not be removed or kept by me when I leave Johns Hopkins except as permitted by Johns Hopkins policies or specific agreements or arrangements applicable to my situation.

It is important that the entire Johns Hopkins Medicine community share a culture of respect for confidential information. To that end, if I observe access to or sharing of confidential information that is or appears to be unauthorized or inappropriate, I will try to make sure that this use or disclosure does not continue. This might include advising the person involved that they may want to check the appropriateness of the use or disclosure with the Johns Hopkins Privacy Officer or the Health System or University Legal Counsel. It may also involve letting my manager (if applicable) or others in authority at the Health System or the University know about the issue or possible issue. Use of the Compliance Hotline (telephone #: 1-877-932-6675) allows this to be done anonymously, if need be. Johns Hopkins may have additional policies regarding procedures for reporting possible inappropriate use or disclosure, and I understand that I must follow these policies, if applicable. I understand that signing this pledge and complying with its terms is a requirement for me to work, volunteer or study at Johns Hopkins.

If I violate this pledge, I will be subject to disciplinary action up to and including termination, severance of volunteer relationship or expulsion from my academic program. In addition, under applicable law, I may be subject to criminal or civil penalties.

I have read the above pledge and agree to be bound by it.

Name: _____ Johns Hopkins Phone: _____

Signature: _____ Date: _____

Social Security Number: _____

Johns Hopkins Dept/School: _____

Confidentiality of Information Statement - Sign and Fax to 4-1798

Management of JHM Information: I understand that I require information to perform my duties. This information concerns the business and operations of JHM that will include Patient Information, Employee Information and the Business Operations of JHM (including Computer Information and Access).

(1) Patient Information: I understand that any patient medical or non-medical information belongs to the patient and that JHM only permits me to access such information to the extent that providing or supporting the provision of patient care in the performance of my duties is necessary. I also understand that all medical and personal information regarding patients is confidential and, unless directly related to the care of patients and authorized by JHM policy, I will not reveal it or discuss it with other patients, friends, relatives, or anyone else within or outside JHM.

(2) Employee Information: I understand that any employee or any patient/employee medical or non-medical information belongs to the employee and that JHM only permits me to access such information to the extent that providing or supporting the provision of employee care in the performance of my duties is necessary. I also understand that all medical and personal information regarding employees is confidential and, unless directly related to the care of employees and authorized by JHM policy, I will not reveal it or discuss it with other employees, patients, friends, relatives, or anyone else within or outside JHM.

(3) JHM Business Operations Information: I understand that any information regarding the business operations of JHM such as financial operations, quality assurance, medical research, risk management, computer security information, etc., belongs to JHM and that JHM only permits me to access such business information to the extent that is necessary in the performance of my duties. I also understand that all operational information is confidential and, unless directly related to my job, and authorized by JHM policy, I will not reveal it or discuss it with any other source including employees, patients, friends, relatives, or anyone else within or outside JHM.

(4) JHM Computer Access: I understand that if issued a computer access security code or codes [USERID(s)], I must keep the code(s) confidential and safeguard them from disclosure to any unauthorized person. Furthermore, if I voluntarily password protect any JHM computer or data files contained within a JHM computer, I will inform my immediate supervisor only of those passwords. I also agree not to access information through any means that JHM policy does not authorize.

I understand that my access security code(s) are only to be used in carrying out my duties. I therefore certify that I will not disclose the codes assigned to me to any other individual nor will I allow any other person to use my codes to access any JHM computing platform. I likewise agree not to use another employee's assigned security code(s) to obtain access to any JHM computing platform or any other equipment even if for the express purpose of performing my duties. I further understand that JHM considers access security codes to be confidential and that any unauthorized disclosure or use of the codes constitutes a breach of that confidentiality.

Since my access security code constitutes the electronic version of my signature, I understand that I will be held accountable for all work performed or changes made to any JHM system or data bases under my security code. As a result, I affirm that I will not permit any other employee to obtain information from a JHM computer system through the use of my access codes; and I will not leave my computer or computer terminal logged on and unattended and/or otherwise available for unauthorized use under my security access code. In the event I believe that the use or confidentiality of my access security code has been compromised, I will immediately inform my supervisor as well as the JHMCIS Security Manager.

I UNDERSTAND IF I VIOLATE THE PROVISIONS OF THIS "CONFIDENTIALITY OF INFORMATION STATEMENT" I WILL BE SUBJECT TO DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION OR REVOCATION OF EMPLOYMENT PRIVILEGES BY JHM ON THE FIRST OR ANY SUBSEQUENT VIOLATION.

Employee Name: _____
(PLEASE TYPE OR PRINT ABOVE)

Employee Signature: _____ Date: _____

Last 4 Digits Social Security #: _____

Department: _____ Title: _____ Phone: _____

Management Witness: _____ Phone: _____ Date: _____