



INFORMATION SERVICES RULES & REGULATIONS

I, the undersigned, acknowledge receipt of these Information Services (IS) rules and regulations and understand that:

1. My IS User Login Name and Password is the equivalent of my signature.
2. I will not disclose any of my IS User Login Names and/or Passwords to anyone.
3. I will not attempt to learn another user's IS User Login Name and Password.
4. I will not attempt to access information by using an IS User Login Name and Password other than my own.
5. I will not attempt to access any unauthorized information via my IS User Login Name and Password.
6. If I have reason to believe that the confidentiality of my IS User Login Name and Password has been compromised, I will contact the Information Services HelpDesk at (516)349-4629 immediately so that the password can be deleted and a temporary password assigned to me, which I will then reset immediately.
7. My IS User Login Name and Password will be deleted from the system as soon as I terminate my employment or association with Episcopal Health Services.
8. I understand that all hardware, software, and computer-related equipment are the property of EHS and are accessible by any EHS IS personnel at any time.
9. Per HIPAA regulations, I will not use my computer to violate any person's privacy, confidential information of any type, or information that compromises internal business.
10. I acknowledge receipt of instructions and/or equipment for HIPAA compliance appropriate to my job description and will conform to EHS policy regarding the use of such instructions and/or equipment.
11. Per HIPAA regulations, I will not jeopardize the physical security of any patient information, either deliberately or through negligence.

Accessing any information without authorization and without a professional need for such information is a breach of the person's rights of confidentiality. Such activity is also deemed to be professional misconduct which could result in the revocation of a license to practice.

Duplication of software without authorization of the manufacturer is a violation of state and federal laws punishable by fine or imprisonment. Installation of any software or changes to configuration on PC's is only to be done by EHS IS personnel in accordance with HIPAA regulations and EHS policies and procedures.

➤ I understand that if I violate any of the above statements I will be subject to disciplinary action in accordance with Human Resources policy.

DEPARTMENT/SITE

EMPLOYEE NAME (please print)

TELEPHONE NUMBER

[* Employee must sign both pages]

DATE

* SIGNATURE OF EMPLOYEE

DATE

WITNESS

[fax to (516) 349-4688]

AUTHORIZATION TO ACCESS SYSTEM

EMPLOYEE'S NAME _____ (print)

DEPARTMENT _____

THESE ARE THE TYPES OF ACCESS, INCLUDING LEVEL OF ACCESS:

ELECTRONIC MEDICAL RECORD ✓

EMAIL ✓ INTERNAL EMAIL _____ EXTERNAL EMAIL _____

PATIENT INFORMATION SYSTEM ✓ (patient inquiry only)

RADIOLOGY ✓

NETWORK ✓ NT ✓

LAB ✓

OTHER _____

House Staff Attending Resident

Intern Student

INSTRUCTIONS FOR SECURITY REQUEST

THIS IS A 2-PART FORM. NO SECURITY ACCESS WILL BE GRANTED UNTIL **BOTH** PAGES ARE COMPLETED. PAGE 1 IS TO BE FILLED OUT BY THE **USER** AND AN APPROPRIATE WITNESS (SUPERVISOR, INFORMATION SERVICES STAFF, SECURITY STAFF, OR EHS MANAGEMENT STAFF). PAGE 2 IS TO BE FILLED OUT BY THE **CHAIRMAN OF SERVICE**. BOTH PAGES ARE TO BE RETURNED TO THE INFORMATION SERVICES DEPARTMENT.
> A NEW SECOND PAGE MUST BE SUBMITTED EACH TIME A NEW SYSTEM IS ADDED TO THE USER'S ACCESS. **CHECK ONLY THE SYSTEM YOU'RE ADDING.**
FOR INITIAL REQUESTS OR TO OBTAIN SPECIFIC INFORMATION, THE DEPARTMENT HEAD SHOULD SEND AN EMAIL TO "SECURITY REQUEST" IN GROUPWISE.

Per Information Services rules and regulations I authorize this user to have access to this system

Chairman of Service Name (please print)

Chairman of Service (signature) Date

* I agree to the I.S. Rules & Regulations for use of the above systems assigned to me

User's Signature

Date