



SECURITY REQUEST FORM

I. Client Information: To be completed by user.

Request Type: [ ] New [ ] Change [ ] Terminate Date:
Employee Type: [ ] Employee [ ] Physician [ ] Volunteer [ ] Agency [ ] Off Site Physician Office
[ ] Student [ ] Instructor [ ] Other
Name (Last): (First): (MI):
Job Title/Position: License (MD, RN, LPN, etc.):
Dept/Office. Phone#: Department Name:
Primary Facility: SSN#: DOB:
Destiny ID: (Required Field)

II. System Information: To be completed by Department Head.

Internal Use Only
Completed By (initials)

Cerner Facilities: [ ] Ormond (93) [ ] Flagler (95) [ ] Oceanside (94) [ ] Deland(96) [ ] Fish(35)
[ ] iConnect Position
Network Access (Windows & Email)
[ ] Network (LAN)
[ ] E-mail
[ ] VPN Access (Managers or Directors Only)
[ ] Other
Series Facilities: [ ] Ormond/Oceanside (93) [ ] Flagler (95) [ ] Deland(96) [ ] Fish(35)
[ ] Department Number Required:
[ ] Menus [ ] Order Supplies [ ] Accounts Receivable Inquiry [ ] CCT
Other Systems
[ ] Dictaphone Contact Transcription Coordinator
[ ] Pyxis Contact Pharmacy
[ ] NextGen Practice: Security Group:
[ ] Horizon [ ] Home Health [ ] Hospice (Home Care)
[ ] Other
[ ] Other

HR/Information Services Use Only:

[ ] Network Logon: Access issued by: Date:
[ ] User Notified How Date:
User H: Drive: Fileserver:
[ ] HBOC Series Access issued by: Date:

Printer Security Code:

III. Please sign and send the original form to HR for NEW HIRES only. Access changes to go to facilities mailroom and MUST include a Destiny ID.

Authorized by: (Print)
(Manager/Director/Supervisor)

(Signature) Signature Required Date: 1/7/10



CONFIDENTIALITY AGREEMENT

NAME:  
(Printed)

\_\_\_\_\_  
Last,

\_\_\_\_\_  
First

\_\_\_\_\_  
Middle Init.

Employee Type:  Employee     Physician     Volunteer     Agency     Off Site Physician Office  
 Student     Instructor     Other    \_\_\_\_\_

I understand that I may be exposed to a variety of clinical, financial, and other types of information generated in the course of business. To assure the integrity of the data, and protect it from accidental loss, alteration, destruction, or tampering by unauthorized individuals, **I agree to the following:**

1. I understand that I will refrain from releasing information (verbally, copies, faxes, downloads or the original record) to individuals who are not authorized to receive this information. This includes refraining from reading the record of or discussing a case/details with coworkers, friends, families, or other associates without a legitimate need to know and/or proper authorization.
2. Any user will and passwords for information systems, and access to information systems which I may be granted access to are strictly confidential, unique to me, and will not be shared with others. I understand these computer key codes are equal to my handwritten legal signature.
3. I understand these codes have been granted to me under a privileged "right to know" and I will limit my access only to the information pertinent to the care of the patient or within the scope of my responsibilities.
4. If I suspect or have knowledge of someone else inappropriately using my password or sign-on I will report this immediately to the Information Services Support Center.
5. All employees shall use software only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes is a violation of the law any unauthorized duplication of copyrighted computer software violates the law and is contrary to the organization's standards of conduct any person illegally copying software other than for backup purposes is subject to appropriate discipline by this organization, and can be subject to civil and criminal penalties including fines and imprisonment. No employee shall give software to outsiders including clients, customers and others. All software used by the organization and company computers will be properly purchased through appropriate procedures. Any employee who determines that there may be a misuse of software within the company shall notify their department manager or Information Services.
6. I have read, understand, and agree to the Information Systems Internet Acceptable Use Policy (600.08).
7. Professionalism should be used in all E-Mail communications, as in any written business communication. Any E-Mail that is in violation of the Hospital's Rules of Conduct or Confidentiality Agreement is prohibited, including but not limited to abusive, profane, derogatory or offensive language and confidential information.
8. I understand this document will be retained on file and that a violation of this policy and/or releasing any confidential information which I am exposed to in the course of my activities can result in limit or termination of access to these systems, change in ID or password assignment, possible disciplinary action, according to hospital policy and/or Medical Staff Rules and Regulations, including termination, and potential liability.

\_\_\_\_\_  
**SIGNATURE**

\_\_\_\_\_  
**DATE**