Clearance Instructions for NTDT412 – Applications in Clinical Practice (Fall 2019)

It is very important to read these directions carefully.

All documentation must be turned into Carrie Johns (contact information below) no later than Friday, August 23, 2019. Not turning in documentation or turning in documentation late could result in a delay in access to the facility for not just you, but the whole class.

REQUIRED DOCUMENTATION:

1. Personal Health Insurance Card (copy of front and back)
2. Background Check
3. Drug Screen
4. Immunization Records
5. PPD Test
6. Flu Shot
7. Screen Shot of Completed Policy & Procedure Quiz (minimum score of 85%)
8. Screen Shot of Completed Pre-Orientation Quiz (minimum score of 100%)
9. Signed Confidentiality Agreement
10. Signed HIPPA-106 Security Oversight
11. Signed Orientation Acknowledgement

BACKGROUND CHECK/DRUG SCREEN:

1. Go online to portal.castlebranch.com/ue74
2. Select Place Order
3. You will be given three package options – select “UE74: Background Check – Drug Test” * ($70.00 Fee**) 
4. Follow the instructions to get set up and create a username and password
   a. Note – Not having a username will result in your background check and drug test results never being reported back.
5. Contact Carrie Johns to schedule a time to pick up a “Chain of Custody Drug Form” for your Drug Test
6. Go to any LabCorp to complete drug test
7. View and download your Background Check/Drug Test results in your CastleBranch profile
8. Turn in result to Carrie Johns

*If you have had a Criminal Background Check completed within the last rolling year, you can use this and select the Drug Screen only option.

**Students are responsible for all fees associated with clearances

IMMUNIZATION/PPD TEST/FLU SHOT:

1. Negative PPD test needs to be valid within the last year (rolling 365 days).
   a. Test can be provided by Student Health ($10.00 fee**) in needed
3. Vaccination Records including
   a. Measles, Mumps, Rubella (MMR) or positive titer
   b. Varicella or positive titer
   c. Hepatitis B (3 shot series) or waiver

These results can be scanned and e-mailed, faxed, or delivered in person to Carrie Johns.

**Students are responsible for all fees associated with clearances
HEALTH INSURANCE CARD

1. Photo of front and back of card sent via e-mail
2. Carrie Johns will photo copy your card if you bring it to her office

ONLINE QUZZES/SIGNED DOCUMENTATION

All of the information for orientation, online quizzes, and signed agreements/acknowledgements are in the attached pages from Union Hospital. Please read these directions carefully and complete all the necessary steps.

CONTACT INFORMATION FOR CARRIE JOHNS

Carrie G. Johns
Cbonnett@udel.edu
Carpenter Sports Building 004

Please let Carrie know when you will be stopping by her office. Please give her your name and tell her which courses you are turning in documentation for.

If she is not in her office, there are envelopes available in the mail-room to put your sensitive documents in. Please use a sticky note to write your name and course number on before placing in her mailbox.

QUESTIONS:

For questions related to course information please contact Prof. Grim (agrim@udel.edu).

For questions related to clearances please contact Prof. Grim or Carrie Johns (cbonnett@udel.edu).
STUDENT EXPERIENCE ORIENTATION

Pre-Requisites – On Site Students and On Site Faculty

Upon confirmation of the sponsor department accepting the Student Experience Candidate(s), each candidate is required to present the following:

- Complete Hepatitis B vaccination series (series of three or waiver)
- Tuberculosis screening (within 12 months)
- MMR vaccination(s) or positive titer(s)
- Varicella vaccination or positive titer
- Influenza vaccination – As Per Current CDC Guidelines.
- Criminal background check completed no more than two (2) years prior to commencement of Student Experience. [ADP package “Criminal Risk”]
- Urine drug screen no more than 6 months prior to commencement of Student Experience
- Personal health insurance
- Complete the following presentations and quizzes on UHCC.COM at the following links
  - Pre-Orientation: https://www.uhcc.com/careers/new-hire-hub/pre-orientation-presentation/
- Confidentiality Agreement
- HIPAA-106 Security Oversight
- Complete Student Emergency Contact form.
- Current professional license (if applicable).

All Pre-Requisites must be received by the Student Experience Coordinator a minimum of fifteen (15) business days prior to start of the Student Experience (weekends and holidays not included).

Student Experience Candidates cannot begin their Student Experience unless these requirements are met and have received a notification from the Student Experience Coordinator of your official clearance.
First Day

Park in the Union Hospital General Employee Parking Lot located on Railroad Avenue, next to Cecil College’s Student Parking Lot.

Please come prepared with two forms of identification.

A representative from the Sponsor department will meet you upon arrival, review identification, and supply you with your ID Badge and show you how to log in at the front desk to track your hours.

During Student Experience

We look forward to providing a positive experience. Throughout your time here your Sponsor Department Representative will be available to assist you with any issues. Please do not hesitate to reach out if you need assistance. You must clock in and out at the front desk in the main lobby to have your Student Experience validated.

Last Day

Please complete the evaluation form to let us know how your Student Experience was.

Your ID Badge should be turned into your Instructor, Sponsor Dept. Point of Contact, or Customer Service.
Employee Parking Guide

- Garage Parking: Patient & Visitor Parking (employees may be eligible, see restrictions above)
- General Employee Parking: All employees eligible (parking permit required)
- Restricted Parking: Patients & Visitors Only
- Permit & Physician Parking Only
- Union Hospital Building

General Employee Parking
Open 24 Hours / 7 Days a Week
(Parking permit required)

No Parking
Cecil College
Parking Only.

Employee Garage
Parking information:
M-F: 7am - 5pm
Sat & Sun: Open
Parking permit required.

Parking Garage
Patient & Visitor Parking
(see employee eligibility above)
The policies set forth do not establish a standard of care to be followed in every case. It is recognized that each case is different and those individuals involved in providing health care are expected to use their clinical judgment in determining what is in the best interests of the patient, based on the circumstances existing at the time. It is impossible to anticipate all possible situations that may exist and to prepare policies for each. Accordingly, these policies should be considered to be guidelines to be consulted for guidance with the understanding that departures from them may be required at times.

**POLICY TITLE:** HIPAA Security Oversight

**POLICY #:** HIPAA-106

Review Responsibility: Anne Lara – Security Officer

Approved By: Laurie Beyer  
Signature/Date: 02/2015  
Original maintained by policy coordinator.

Effective: 04/2005  
Reviewed: 08/2012, 02/2012, 08/04/17  
Revised: 01/01/2015, 08/2012, 02/2012, 02/2015  
Scope: All Staff

I. **Purpose:**  
To provide for the appropriate development, implementation, and oversight of Union Hospital’s efforts toward compliance of the HIPAA security regulations

II. **Policy Statement: Definitions:**  
In accordance with the standards set forth in the HIPAA Security Rule, Union Hospital is committed to ensuring the confidentiality, integrity, and availability of all electronic protected health information (e-PHI) it creates, receives, maintains, and/or transmits. Union Hospital has a HIPAA Security Officer [164.308(a)(2)] responsible for facilitating the training and supervision of all workforce members [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any workforce member that is in non-compliance with the HIPAA security regulations [164.308(a)(1)(ii)(c)], and writing, implementing, and maintaining all policies, procedures, and documentation related to efforts toward HIPAA security compliance [164.316(a-b)].

III. **Definition:**

| **Electronic Protected Health Information (e-PHI)** | Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media. |
| **Protected Health Information (PHI)** | Individually identifiable health information that is created by or received by the organization, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:  
· Past, present or future physical or mental health or condition of an individual.  
· The provision of health care to an individual. |
<table>
<thead>
<tr>
<th>Workforce</th>
<th>The past, present, or future payment for the provision of health care to an individual.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workforce</td>
<td>Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.</td>
</tr>
</tbody>
</table>

IV. **Approach/Philosophy:**

**HIPAA Security Officer Responsibilities.** The HIPAA Security Officer, in collaboration with the HIPAA Privacy Officer (if not held by the same individual), is responsible for facilitating the development, implementation, and oversight of all activities pertaining to Union Hospital’s efforts to be compliant with the HIPAA Security Regulations. The intent of all oversight activities includes those necessary to maintain the confidentiality, integrity, and availability of e-PHI. These responsibilities are included in the HIPAA Privacy/Security Officer’s job description (see Compliance and Privacy Practices) and include, but are not limited to the following:

a) Oversees and enforces all activities necessary to comply with the Security rule and verifies the activities are in alignment with the requirements.

b) Establishes and maintains written policies and procedures to comply with the Security rule and maintains them for six years from the date of creation or date it was last in effect, whichever is later.

c) Updates policies and procedures as necessary and appropriate to comply with the Security rule and maintains changes made for six years from the date of creation or date it was last in effect, whichever is later.

d) Facilitates audits to validate Security compliance efforts throughout the organization.

e) Documents all activities and assessments completed to comply with the Security rule and maintain it for six years from the date of creation or date it was last in effect, whichever is later.

f) Provides copies of the policies and procedures to management, and has them available to review by all other workforce members to which they apply.

g) Annually, and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security of e-PHI.

h) Reviews annual training for all workforce members of established policies and procedures as necessary and appropriate to carry out their job functions.

i) Develops and provides periodic security updates to the Affinity Health Institute for reminder communications for all workforce members.

j) Implements procedures for the authorization and/or supervision of workforce members who work with e-PHI or in locations where it may be accessed.

k) Maintains a program promoting workforce members to report non-compliance with established Security rule policies and procedures. (See Occurrence Reporting Process AG-240)
i) Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.

ii) Applies consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Union Hospital.

iii) Mitigates to the extent practicable, any harmful effect known to Union Hospital of a use or disclosure of e-PHI in violation of Union Hospital’s policies and procedures or business associates.

l) Reports security efforts and incidents to administration in a timely manner.

m) Assists in the administration and oversight of business associate agreements.

Workforce Training.

a) The HIPAA Security Officer facilitates the training of all workforce members as follows:

i) Supplies to Human Resources necessary materials for New Employee Orientation

ii) Supplies to the Affinity Health Institute department the material for annual competency training.

iii) Notification to workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective.

b) Ensure that workforce members sign into the training session.

c) Ensures that Human Resources and/or department manager retains documentation of the training session materials and attendees for a minimum of six years.

d) The training session focuses on, but is not limited to, the following subjects defined in Union Hospital’s security policies and procedures (such as the System Access policy and Communication of PHI policy):

i) Auditing. Union Hospital may monitor access and activities of all users

ii) Workstations may only be used to perform assigned job responsibilities

iii) Users may not download software onto Union Hospital’s workstations and/or systems without prior approval from the HIPAA Security Officer

iv) Users are required to report malicious software to the HIPAA Security Officer immediately

v) Users are required to report unauthorized attempts, uses of, and theft of Union Hospital’s systems and/or workstations

vi) Users are required to report unauthorized access to facilities

vii) Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation)

viii) Users may not alter e-PHI maintained in a database, unless authorized to do so as a part of their job responsibilities

ix) Users are required to understand their role in Union Hospital’s contingency plan

x) Users may not share their user names nor passwords with anyone

xi) Requirements for users to create and change passwords
xii) Users must set all applications that contain or transmit e-PHI to automatically log off after 10 minutes of inactivity.

xiii) Managers are required to report terminations of workforce members and other outside users.

xiv) Managers are required to report a change in a user’s title, role, department, and/or location

xv) Procedures to dispose of discs, cd, hard drives, and other media containing e-PHI.

xvi) Procedures to re-use electronic media containing e-PHI.

xvii) Email encryption procedures

e) The HIPAA Security Officer facilitates the communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:

i) Latest malicious software or virus alerts

ii) Union Hospital’s requirement to report unauthorized attempts to access e-PHI

iii) Changes in creating or changing passwords

f) Additional training is provided to workforce members in the information services department. This training is specific in nature, as to the Union Hospital’s requirements for their involvement in areas such as the following:

i) Data backup plans

ii) System auditing procedures

iii) Redundancy procedures

iv) Contingency plans

v) Virus protection

vi) Patch management

vii) Media Disposal and/or Re-use

viii) Documentation requirements

Supervision of Workforce. Although the HIPAA Security Officer is responsible for implementing and overseeing all activities related to compliance with the Security rule, it is the responsibility of all leaders (i.e. team leaders, supervisors, managers, directors, etc.) to supervise all workforce members and any other user of Union Hospital’s systems, applications, servers, workstations, etc. that contain e-PHI.

a) Leaders monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.

b) Leaders assist the HIPAA Security Officer to ensure appropriate role-based access is provided to all users.

c) Leaders take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and Union Hospital’s security policies and procedures.
Sanctions. All workforce members and other users report non-compliance of Union Hospital’s policies and procedures to the HIPAA Security Officer or other individual as assigned by the HIPAA Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence. (Refer to HR-323 Anti-Retaliation Policy and Compliance and Privacy Practices for additional information).

a) The HIPAA Security Officer promptly facilitates a thorough investigation of all reported violations of Union Hospital’s security policies and procedures. The HIPAA Security Officer may request the assistance from others such as Human Resources, the workforce member’s or users’ leader, other workforce members, and/or other users.

i) Complete an audit trail/log to identify and verify the violation and sequence of events.

ii) Interview any individual that may be aware of or involved in the incident.

(1) All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.

(2) Provide individuals suspected of non-compliance of the Security rule and/or Union Hospital’s policies and procedures the opportunity to explain their actions.

iii) The investigators thoroughly document the investigation as the investigation occurs.

b) Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers’ offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations. Refer to Union Hospital’s Constructive Discipline Policy.

i) Below describes the sanctions that will be applied based on access offense:

Employees (excluding employed providers)

a. First Offense: Written Warning

b. Second Offense: Suspension without pay for 24 working hours

c. Third Offense: Termination of Employment

Medical Staff (including employed providers) (the Medical Executive Committee, or UHCC, in the case of employed providers) may choose to impose more severe sanctions under appropriate circumstances)

a. First Offense: Written Warning

b. Second Offense: Three (3) business day suspension of access to the EMR plus $1,000 fine (access not restored until fine is paid)

c. Third Offense: Termination of Medical Staff privileges

c) UHCC reserves the right in all instances to take measures appropriate to the circumstances, including imposing more severe discipline than as outlined above if a
HIPAA violation is committed with wrongful or malicious intent or results in harmful effects.

D) All instances of improper access, i.e., accessing another individual’s record for purposes other than performing a job function, are required to be reported to the Office for Civil Rights of the U.S. Department of Health and Human Services as HIPAA breaches.

E) The HIPAA Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).

F) The HIPAA Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.

V. References:
   i. HIPAA 164.308(a)(1)(ii)(c), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(5), 164.316(a-b)
I. Purpose:
It is the policy of Affinity Health Alliance and Union Hospital that all employees and associates (volunteers, vendors, Board Members, and other individuals affiliated with the hospital understand the organization’s commitment and his/her role and responsibility as it relates to patient, customer, hospital, employee confidentiality and complies as required by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

II. Policy Statement:
General Rule: We expect all employees, vendors and associates to maintain information in a confidential manner, including patient information and diagnosis, employee information, financial data and operational policies, procedures, plans and information. It is important that any and all computer based systems that have patient or employee information, should not be used to gather information about employees or patients except in their official capacities.
III. Definition:

**Confidentiality:** The legally protected right afforded to (and duty required of) specifically designated health care professionals not to disclose information discerned or communicated during consultation with a patient.

**Protected Health Information (PHI):** Individually identifiable health information that is created by or received by the organization, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

**Vendors:** persons from other organizations marketing or selling products or services, or providing services to Union Hospital. Examples include, but are not limited to the following:
1. Pharmaceutical Representatives,
2. Equipment Repair Service Personnel,
3. Food Services, and
4. Independent Contractor for Union Hospital.

**Workforce:** As defined in the HIPAA Privacy Rule, employees, volunteers (board members, community representatives), trainees (students), contractors, and other persons under the direct control of a covered entity.

IV. Approach/Philosophy:

During employment and/or association with Affinity Health Alliance and Union Hospital, employees and associates have access to many types of confidential information, including patient information and diagnosis, employee information,
financial data and operational policies, procedures, plans and information. All associates have both a legal and an ethical obligation to protect sensitive data.

All potential candidates must sign the confidentiality statement when attending job shadow.

**During the new-hire process and as part of Annual Review, every employee shall sign a confidentiality statement as attached to the Annual Review,** acknowledging his/her understanding of Affinity Health Alliance’s commitment and the employee’s responsibility as it relates to the protection of patient, employee and customer information. This confidentiality statement also addresses an employee’s responsibility to alert appropriate staff of any possible concerns surrounding Compliance.

Except as directed by the Board of Directors and/or the President and CEO, employees, vendors and associates may not, at any time, access or disclose any information to any person whatsoever or permit any person whatsoever to examine or make copies of reports or documents that contains Protected Health Information (“PHI”), except with a signed Release of Information process or pursuant to legal obligations through the summons process (both clinical and non-clinical information), employees, financial, strategic, program or operational information of Affinity Health Alliance. Employees and associates may not seek any confidential information concerning patients (both clinical and non-clinical information), employees, financial information or operational information except as required in the performance of their duties.

Because of the critical nature of confidentiality within our organization, processes have been put into place to investigate any possible violations of this policy. Random audits of patient records and employees access of patient records both onsite and offsite will be performed regularly. Also any suspected violations will be investigated and appropriate action will be taken, up to and including termination and/or other legal remedies.

**Related Documents/Policies:**

a. Confidentiality Agreement
# Student Experience Orientation

Information Sheet:  
- [ ] Student  
- [ ] On Site Faculty

<table>
<thead>
<tr>
<th>Unit</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
</table>

| Name: | |
| Phone: | Primary | EMAIL | @ |

| Address | Street | City | State | Zip |

## School Information

| Name | |
| Address | City | State | Zip |

| Faculty Advisor | |

| Program | Name | Level |

## Emergency Contact Information – 1 REQUIRED

| Name: | |
| Phone: | Primary | Secondary |

| Relationship | |

| Name: | |
| Phone: | Primary | Secondary |

| Relationship | |

I attest that the above information is correct:

Signature: ___________________________ Date: __________
Confidentiality Agreement

I agree to protect the confidentiality, privacy and security of patient, student, staff, business and other confidential, sensitive electronic or proprietary information (collectively, “Confidential Information”) of Union Hospital of Cecil County and all Affiliated Providers from any source and in any form (spoken, paper, electronic). I understand that I have an obligation to protect the Confidential Information that I may create, access, use or disclose as part of my job including the following, among others:

- **PATIENTS AND/OR FAMILY MEMBERS** (such as, patient records, conversations and billing information)
- **MEDICAL STAFF, EMPLOYEES, VOLUNTEERS, STUDENTS, or CONTRACTORS** (such as, social security numbers, salaries, clinical information, billing information, employment records, disciplinary actions)
- **BUSINESS INFORMATION** (such as, financial records, research or clinical trial data, reports, contracts, computer programs, technology)
- **THIRD PARTIES** (such as, vendor contracts, computer programs, technology)
- **OPERATIONS, PERFORMANCE IMPROVEMENT, QUALITY ASSURANCE, MEDICAL OR PEER REVIEW** (such as, utilization, data reports, quality improvement, presentations, survey results)

I AGREE THAT:
1. I WILL protect Union Hospital Confidential Information in any form. I WILL follow federal and state statutes and regulations and Union Hospital Policies, procedures and other privacy and security requirements (“Union Policies”).
2. I WILL NOT post, discuss, or otherwise share any Confidential Information, including patient pictures or videos, financial or personnel information on any social media sites such as Facebook or Twitter. I WILL NOT post Confidential Information including patient information or pictures on Union-sponsored social media sites without the appropriate patient authorization in accordance with management approval and Union Policies and procedures.
3. I WILL NOT take any pictures of patients for personal use with any device of any kind.
4. I WILL complete all required privacy and security training.
5. I WILL ONLY access information that I need to perform my job responsibilities or services at Union.
6. I WILL NOT access, show, tell, use, release, e-mail, copy, give, sell, review, change or dispose of Confidential Information unless it is part of my job responsibility or to provide service at Union. I WILL follow Union Policies (such as shredding confidential papers using confidential shred containers/lock bins or deleting electronic files from devices) and only access/use the minimum necessary of the information to complete the required task.
7. When my work or service at Union ends, I WILL NOT disclose any Confidential Information, and I WILL NOT take any Confidential Information with me if I leave or I am terminated.
8. If I must take Confidential Information off Union property, I WILL do so only with my supervisor’s permission and/or in accordance with Union policies and procedures. I WILL protect the privacy and security of the Confidential Information in accordance with Union Policies and I WILL return it to Union.
9. If I have access to Union computer system(s), I WILL follow the Secure System Usage Process.
10. I WILL NOT use another’s User ID or password to access any Union electronic or other system, and I WILL NOT share my User ID or password or other computer passwords with anyone.
11. I WILL create and change a strong password** in accordance with Union Policies. I WILL notify the Privacy Officer and change my password at once if I think someone knows or used my password. I WILL ask my supervisor if I do not know how to change my password.
12. I WILL tell my supervisor and the Privacy Officer if I am aware of any possible breaches of my user name or password. I WILL report suspected breaches of confidentiality to my supervisor and the Compliance Officer.
13. I WILL log out or secure my workstation when I leave the computer unattended.
14. I WILL ONLY access Confidential Information at remote locations in accordance with Union Policies.
15. If I am allowed to remotely access Confidential Information, I AM RESPONSIBLE for ensuring the privacy and security of the information at ANY location (e.g., home, office, etc.).
16. With the exception of accessing Union email on a personal smartphone (e.g., iPhone or Android device), tablet (e.g., iPad), or similar device, I WILL NOT store Confidential Information on non-Union systems including on personal computers/devices, in accordance with the mobile device policy. I WILL immediately report any lost or stolen device, personal or otherwise, that was used to access Union resources.
17. I WILL NOT maintain or send Confidential Information to any unencrypted mobile or portable storage device in accordance with Union Policies.
18. I UNDERSTAND that my access to Confidential Information and my Union e-mail account may be audited.
19. If I receive personal information through Union e-mail or other Union systems, I AGREE that authorized Union personnel may examine it, and I do not expect it to be protected by Union.
20. I UNDERSTAND that Union may remove or limit my access to Union’s computer system(s) at any time.
21. I understand that I must report any identity theft of my personal information to the Compliance Officer as soon as I am aware of the occurrence.

I understand that my failure to comply with this Agreement may result in the termination of my relationship with Union and/or civil or criminal legal penalties. By signing this, I agree that I have read, understand, and WILL comply with this Agreement.

Signature: ___________________________________________ Date: __________________________

Print Full Name: ________________________________________ Dept.: ________________________

Created 1/2016

Page 1 of 2
Examples of Breach of Confidentiality
(What you should NOT do)

These are examples only. They do not include all possible breaches of confidentiality covered by the Union Breach of Protected Health Information/Patient Privacy policy and this Confidentiality Agreement.

Accessing information that you do not need to know to perform Your job responsibility or services:

• Unauthorized reading of patient account information.
• Unauthorized reading of a patient’s chart.
• Accessing information on adult children, friends or co-workers.

Sharing, copying or changing information without proper authorization:

• Making unauthorized changes to an employee file.
• Discussing Confidential Information in a public area; such as, a waiting room, elevator, or cafeteria.
• Posting a picture of a patient on a social media site.
• Commenting on a patient on a social media site.

Sharing your User ID and password:

• Sharing your password so a co-worker can log into Union’s computer system(s) to do their work or yours.
• Giving someone the access codes for employee files or patient accounts.
• Emailing confidential information outside of Union by unsecure methods (not encrypted).

Leaving a secured application*** unattended while signed on:

• Being away from your computer while you are logged into patient billing information.
• Allowing someone to access Confidential Information using your User ID and password.

DEFINITIONS

* Secure System Access Policy – HIPAA Policy #101 - Posted on the Union Hospital Intranet provides an overview of the information security policies, standards, and procedures that apply to all Union Hospital staff, students, and affiliates.

** Strong Computer Passwords are defined in the HIPAA Policy #101 and must be in accordance with Union HIPAA Security policies.

*** Secured Application – any computer program that allows access to Confidential Information. A secured application usually requires a user name and password to log in.
# STUDENT EXPERIENCE ORIENTATION

## ACKNOWLEDGEMENT — YOU MUST INITIAL EACH LINE!

**STUDENT NAME:** ________________________________

<table>
<thead>
<tr>
<th>Initials</th>
<th>Topics</th>
<th>Objectives</th>
</tr>
</thead>
</table>
|          | Welcome/Corporate Goals       | • Awareness of Organizational Goals  
                                      • Understanding to Hospital’s mission and vision                                      |
|          | Organizational Values         | • Understand actions and practices of Core Values  
                                      • Group Interaction – Employee Choice Award                                                |
|          | Patient Safety                | • What is a Safety Event  
                                      • What should be reported  
                                      • How to report an event  
                                      • Quantros  
                                      • **SPEAK UP & BE SAFE** Dial **SAFE** x (7233)  
                                      • Why Report                                                                         |
|          | Infection Prevention          | • Importance of hand washing  
                                      • PRECAUTIONS: Standard, Contact, Droplet  
                                      • MRSA  
                                      • Isolation Red Box  
                                      • Employee Exposure  
                                      • Hospital Inquired Infections                                                        |
|          | Compliance / HIPAA            | • HIPAA – Federal Law of 1996  
                                      • HIPAA Policy 106  
                                      • Compliance information  
                                      • Safeguards  
                                      • Impact of breach  
                                      • Patient Portal                                                                    |
|          | Service Excellence            | • Meaning of Service Excellence  
                                      • Company Culture  
                                      • CLUE  
                                      • Language of Caring                                                                 |
<table>
<thead>
<tr>
<th>Initials</th>
<th>Topics</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Emergency Preparedness / Safety</td>
<td>• Who has a role</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• What is your role</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Safety Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Workplace Violence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hazardous Materials &amp; Waste</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Equipment Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Utilities Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fire Safety</td>
</tr>
<tr>
<td></td>
<td>On-line review of Policies and Procedures</td>
<td>• Emergency Preparedness</td>
</tr>
<tr>
<td></td>
<td>and where to locate policies on intranet</td>
<td>• Employee Cultural, Ethical &amp; Religious Values – HR 309</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Patient’s Rights and Responsibilities – AG245</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Patient Safety and Care</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Corporate Compliance Plan / Code of Conduct / Harassment</td>
</tr>
</tbody>
</table>

_I HAVE, READ, REVIEWED AND UNDERSTAND THIS INFORMATION COVERED IN THE STUDENT EXPERIENCE ORIENTATION. I AGREE TO PERFORM THESE TASKS AND OTHERS AS ASSIGNED OR DIRECTED BY UNION HOSPITAL OF CECIL COUNTY TO THE BEST OF MY ABILITIES._

<table>
<thead>
<tr>
<th>STUDENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printed Name</td>
</tr>
<tr>
<td>Signatures</td>
</tr>
</tbody>
</table>

Initialed and signed document must be sent electronically to the Student Experience Coordinator.