Documents for Accepted Students
2019 - 2020 Academic Year

Gateway Community College
20 Church Street
New Haven, CT 06510

Please note: this information is ONLY for accepted students to the CT-CCNP for the 2019-2020 academic year.
April 2019

Dear Nursing Student,

Congratulations on your acceptance to the Connecticut Community College Nursing Program (CT-CCNP) at Gateway Community College (GCC). Please review the accompanying attachments for important dates and information on the acceptance process.

A mandatory orientation session will be held on Wednesday, June 5th from 4:00PM – 6:00PM in Room N100. This session will provide an overview of the program and information on important dates and materials.

All Health Assessment Forms must be completed by your Healthcare Provider and uploaded to CastleBranch, a confidential document tracking system by June 21, 2019. Instructions for order placement are attached.

Students are required to provide documentation of current professional level certification in Basic Life Support for adult, child, and infant by June 21, 2019. Certification can only be earned through the American Heart Association or the American Red Cross and must remain current throughout the program. Please see attached flier for courses available at GCC.

Our clinical partners require background checks and toxicology screening for nursing students entering their facilities. To comply with this mandate, the CT-CCNP at GCC is requiring you to have a CORE background check and a twelve panel drug screen coordinated by The Connecticut League for Nursing. Information on these two requirements will be provided to you at your advisement appointment.

In order for you to participate in nursing clinicals, you must score an 85% or higher on the Connecticut Hospital Association (CHA) Health and Safety Training Course and the Yale-New Haven Health HIPAA: Information Security for Health Care Workers. Instructions on how to access the CHA Course are attached. The HIPAA packet is also attached. A scantron form will be distributed out at your advisement session for you to place the answers to the test questions.
Also, included in the Accepted Student Documents packet is the Scrub Wear House flier. You can purchase your uniforms for clinical at any Scrub Wear House location. Please mention to the Scrub Wear House staff that you are an accepted GCC Nursing student and you will be directed to the correct uniform. All students must purchase a lab coat, scrub top and pants.

On behalf of the entire nursing faculty and staff at Gateway Community College, I congratulate you on your acceptance and I welcome you to the nursing program. We wish you much success and look forward to meeting you in June.

Sincerely,

Sheila Solernou, RN, MSN
Division Director, Allied Health and Nursing
Mandatory General Nursing Orientation
Wednesday, June 5, 2019
4:00PM – 6:00PM
Room N100

Mandatory Nursing Orientation Workshops
Tuesday, July 30, 2019
Wednesday, July 31, 2019
Thursday, August 1, 2019
3:00PM – 7:00PM
Room N100

**Accepted Students must attend both the mandatory general orientation and the three orientation workshop sessions to retain their seat in the nursing program**
**LPN Mandatory Orientation**

Monday, May 6, 2019  
4:00-6:00PM  
Room S424

**Mandatory Nursing Orientation Workshops**  
For Accepted LPN Students

Monday, August 19, 2019  
Tuesday, August 20, 2019  
Wednesday, August 21, 2019  
3:00 – 7:00PM  
Room S412
CHANGE OF CURRICULUM

STUDENT I.D. @ _______________________________ DOB _______/_____/_____

NAME ____________________________________________________________

ADDRESS ________________________________________________________

CITY/STATE ______________________________________________________

FROM: General Studies

TO: Nursing OPTION: ________________________________

Student Signature ___________________________ Date __________

Coordinator Signature* _______________________ Date __________

Counselor/Advisor Signature __________________ Date __________

*Coordinator's signature required for Automotive, Dietetic, DARC, Human Services and Radiology Technology programs.

Registrar Office Only: H.S. Transcript/GED _______________________

Immunization Doc ____________________________________

Data Entry Date _______________________________________

REVISED 2/17
Be a LIFE SAVER
American Heart Association Basic Life Support for the Healthcare Providers

Register Now - Limited Seats Available

In this classroom-based course, healthcare professionals learn to recognize several life-threatening emergencies, provide CPR to victims of all ages, use an automatic external defibrillator (AED), and relieve choking in a safe, timely and effective manner.

- Critical concepts of high-quality CPR
- The American Heart Association Chain of Survival
- 1-Rescuer CPR and AED for adult, child and infant
- 2-Rescuer CPR and AED for adult, child and infant
- Differences between adult, child and infant rescue techniques
- Bag-mask techniques for adult, child and infant
- Rescue breathing for adult, child and infant
- Relief of choking for adult, child and infant

<table>
<thead>
<tr>
<th>CRN</th>
<th>DAY</th>
<th>DATE</th>
<th>TIME</th>
<th>ROOM</th>
</tr>
</thead>
<tbody>
<tr>
<td>2131</td>
<td>Monday</td>
<td>April 8</td>
<td>5:00 PM-10:00 PM</td>
<td>N005</td>
</tr>
<tr>
<td>2132</td>
<td>Wednesday</td>
<td>April 24</td>
<td>9:00 AM-2:00 PM</td>
<td>N005</td>
</tr>
<tr>
<td>2133</td>
<td>Thursday</td>
<td>April 25</td>
<td>5:00 PM-10:00 PM</td>
<td>N005</td>
</tr>
<tr>
<td>2134</td>
<td>Wednesday</td>
<td>May 1</td>
<td>9:00 AM-2:00 PM</td>
<td>N005</td>
</tr>
<tr>
<td>2136</td>
<td>Wednesday</td>
<td>May 15</td>
<td>9:00 PM-2:00 PM</td>
<td>N005</td>
</tr>
</tbody>
</table>

AHA Disclaimer: Use of American Heart Association materials in an educational course does not represent course sponsorship by the American Heart Association. Any fees charged for such a course, except for a portion of fees needed for AHA course materials; do not represent income to the Association.
All Top Brands: Cherokee, Barco, Dickies, and so much more...
Widest Selection, Outlet Prices
Custom Logo Embroidery
Online Ordering
Group Sales

860-571-8966
info@scrubwearhouse.net
www.scrubwearhouse.net

Visit Our Convenient Locations
Stores Open
Monday thru Saturday 10 AM - 6 PM
Thursday till 8 PM
Sunday 11 AM - 4 PM

Shop Online and Choose
Home Delivery or In Store Pick-Up

Massachusetts
2275 Northampton Street
Holyoke, MA 01041
PH: 413-552-3700

Connecticut
2409 Main Street
Rocky Hill, CT 06067
PH: 860-571-8966

195 Chase Avenue
Waterbury, CT 06704
PH: 203-527-0818

232 Boston Post Road
Milford, CT 06460
PH: 203-877-1293
Submitting Documents

Submitting documents to myCB can be achieved three ways: via upload, fax, or mail. This guide will cover all three options. If you need any further assistance, please call the number located at the bottom right of every page.

UPLOADING DOCUMENTS

The most efficient way to submit. Uploading your documents through myCB is not only secure, but ensures faster processing time.

Options for Digitizing Your Document

- Take a picture
- Use the myCB app
- Scan your document
- Utilize a local FedEx, UPS, Library, or University’s resources

Submitting Through myCB

- Click **To-Do Lists** within the myCB panel on the left
- Expand the requirement you wish to upload to
- Click **Browse** next to **Your Computer or Flash Drive**
- Select file(s) needed, one at a time
- Hit **Submit**

**Note:** Document removal may only happen before submission. Make sure you have attached the correct file name(s) before submitting. To remove a document, simply click **Remove Document** and re-attach the correct version.

Replacing Rejected Documents

- Read the rejected reason
- Re-upload using the same steps above

**The two most common rejection reasons are missing information and illegible documentation.** Make sure your documents are easily legible and contain their essential information, such as: signatures, physical exam dates, vaccination dates, or titer collection dates.
Submitting Documents

FAXING DIRECTLY TO REQUIREMENTS

Following the steps below will result in your documents automatically attaching to their specific requirements, designated by their included cover letters.

Print Cover Letters

1. Click To-Do Lists within the myCB panel on the left
2. Expand the requirement you wish to upload to
3. Click Download at the bottom
4. Read and close the warning prompt
5. Print the cover letter
6. Follow the directions on the cover sheet
7. Repeat for all requirements to be faxed

FAXING TO DOCUMENT CENTER

Following the steps below will result in your documents going into your myCB document center, where you will need to attach them to each requirement individually.

Print Cover Letter

1. Click Document Center within the myCB panel on the left
2. Click Print/Fax Mail Cover Sheet on far right
3. Read and close the warning prompt
4. Print the cover sheet
5. Follow the directions on the cover sheet
6. Faxed documents will display under My Documents within the Faxed folder

Submit Through myCB

1. Click To-Do Lists within the myCB panel on the left
2. Expand the requirement you wish to upload to
3. Click Browse next to My Documents
4. Choose the Faxed folder
5. Pick document needed
6. Hit Submit
Submiting Documents

MERGING FAXED PAGES

If submitting more than one document to a requirement, you have the option to merge them together.

To Merge Pages

1. Click Document Center
2. Find the Faxed/Mailed Documents folder
3. Select one file you wish to merge with another
4. Click Add PDF to Merge Queue
5. Repeat until all pages you wish to merge are queued
6. Select Merge These Documents at the top right
7. All merged files can be found in the Merged Files folder.

MAILING DOCUMENTS TO CASTLEBRANCH

Follow the steps below to mail documents to CastleBranch for review.

Print Cover Letters

1. Click To-Do Lists within the myCB panel on the left
2. Expand the requirement you wish to mail in
3. Click Download at the bottom
4. Read and close the warning prompt
5. Print the cover letter
6. Repeat for all requirements to be sent in
7. Mail to: CastleBranch
1844 Sir Tyler Drive
Wilmington, NC 28405
Attn: TDL Document Center

Note: Pages mailed to CastleBranch should be ordered accordingly:

- Cover letter A, document A
- Cover letter B, document B
Welcome to myCB!

When you place your initial order, you will be prompted to create your secure myCB account. From within your myCB, you will be able to:

✔ View your order results
✔ Manage requirements specific to your programs
✔ Complete tasks as directed to meet deadlines
✔ Upload and store important documents and records
✔ Place additional orders as needed.

To place an order, go to mycb.castlebranch.com

In the “Place Order” field, enter the following package code specific to your organization:

GC57im : Medical Document Manager

During order placement you will be asked for personal identifying information needed for security or compliance purposes. Supplying accurate and comprehensive information is important to the speed in which your order is completed.

The email address you use when placing your order will become your username for your myCB and will be the primary form of communication for alerts and messages. Payment methods include: MasterCard, Visa, debit card, electronic check, money order, and installment payment.

You can respond to any active alerts or To-Do List items now, or return later by logging into your myCB. You will receive alerts if information is needed to process your order. Access your myCB anytime to view order status and completed results. Authorized users at your organization will have access to view your compliance status from a separate CastleBranch portal.
GATEWAY COMMUNITY COLLEGE
STUDENT NURSES ASSOCIATION

CONGRATULATIONS INCOMING STUDENT NURSES!

The members of SNA would like to invite you to opportunities in leadership development and community outreach. We encourage you to contact us with questions or suggestions by emailing gw-sna@gatewayct.edu and/or joining our Facebook group “GCC SNA”

SPRING 2019 MEETING DATES

MARCH 6 2PM
MARCH 26 1PM
APRIL 8 1PM
LOCATION: S109

BAKE SALES

FAIRWAY
10AM – 2PM
MARCH 21
APRIL 23
2019 Connecticut Health & Safety Training Course

Please complete the Health & Safety Training Course and test by accessing the following link:

HIPAA:
Information Security for Health Care Workers
Overview of the HIPAA security requirements

In February 2003, the HIPAA security rule was announced. The regulation becomes enforceable for most covered entities on April 21, 2005.

The regulations are designed to safeguard electronic protected health information (PHI). The rule covers information stored on hard drives, removable or transportable digital memory medium, such as magnetic tape or disk, and information being transported electronically via the Internet, e-mail, or other means. It does not cover fax or voice telephone transmission.

In this course, you will learn about the key measures you can take in your day-to-day work to protect electronic PHI. Although your organization has put in place many technical and policy safeguards to secure its patients’ health information, those investments are useless without the cooperation and support of everyone who must use the organization’s computers. Ultimately, you are the key to your organization’s compliance with the HIPAA security rule.

Covered entities

All HIPAA "covered entities" must comply with the security rule. Covered entities are health plans, health care clearinghouses, and provider organizations that transmit patient information electronically. Provider organizations include most physician and other independent practices providing health care, ambulatory facilities, hospitals, nursing homes, home health care agencies, and any other health care provider. As someone who will work with health information, it’s important for you to know what your responsibilities are under this rule.

Chances are good that you have already received training about the HIPAA privacy rule. As you read this handbook you will notice that the security measures discussed represent, in large measure, the mechanisms that support the efforts to protect privacy that are already in place.
What is information security?

The term security in this context refers to all the protections in place to ensure that information is kept confidential, that it is not improperly altered or destroyed, and that it is readily available to those who are authorized. These principles—confidentiality, integrity, and availability of data—represent the heart of any information security program. Your organization’s security program addresses a broad number of requirements, including:

- computer hardware
- software
- personnel policies
- physical security
- information practice policies
- disaster preparedness
- oversight of all these areas

But all the policies and procedures in these areas work toward the same goal: protecting the confidentiality, integrity, and availability of information.
What are we protecting?

Your organization has many types of information that it must secure, but HIPAA places a special emphasis on PHI. HIPAA specifically gives the patient a certain degree of control over his or her medical records. This includes, to some extent, who views it, who uses it, and where their PHI may be sent. PHI can include anything that can be used to identify a patient, including a patient's:

- name
- address
- Social Security number
- phone number
- condition
- date of surgery

Inappropriately accessing or releasing this information can be a HIPAA violation, and can violate a patient's privacy or affect a patient's care, which is why securing the information within your organization is essential.

Federal penalties for noncompliance

Poor information security practices can lead to security and privacy violations under HIPAA. These can lead to large fines and even jail time for the most serious offenses, i.e., those that lead to personal monetary gain.

HIPAA outlines the following criminal penalties for individuals and organizations who knowingly and wrongfully disclose patient information:

- Misuse of personally identifiable health information. Penalty: Fines up to $50,000 and/or imprisonment for a term of up to one year.
- Misuse under false pretenses. Penalty: Fines up to $100,000 and/or imprisonment for a term of up to five years
- Misuse with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Penalty: Fines up to $250,000 and/or imprisonment for a term of up to 10 years.
Sanctions

Your organization takes the responsibility to secure the PHI in its care seriously. You must also take that responsibility seriously. Failure to adequately protect the security of your organization's PHI can result in disciplinary action being taken against you, up to and including dismissal, termination of business contract, and reporting the violation to licensing agencies and law enforcement officials. That's not meant to intimidate, but simply to emphasize that your security responsibilities are important. If you have any security-related questions about practices that you or others in the organization are carrying out, don't hesitate to ask your supervisor/information security officer.

YNHHS HIPAA Policy Summary: Appropriate Use of Electronic Resources

YNHHS workforce members are required to use YNHHS’ electronic resources in a professional, lawful and ethical manner, and to prevent the unauthorized use or disclosure of protected health information or any other confidential information. Use of electronic resources will be subject to managerial review and based on job requirements.

Key Points

1. YNHHS can monitor the use of the resources with available technologies, with or without the knowledge of the member of the workforce, with the exception of phone conversations.
2. Electronic Resources include, but are not limited to: Personal Computers, E-mail, Voicemail, Telephones, Fax Machines, Pagers, Laptops, Cell Phones, Copiers, and PDAs.
3. Some examples of inappropriate behavior that should be reported to the Information Security Officer and/or the Office of Privacy and Compliance and that warrant disciplinary actions up to and including termination are:
   - Using someone else’s password or login ID.
   - Unauthorized viewing or use of PHI or confidential information.
   - Unauthorized access to system, data or hard copy information.
   - Unauthorized transmission of protected health information (PHI) or confidential data over the Internet (for example, unencrypted transmission of a patient’s medications)
   - Breach of external networks (for example, firewalls, web servers and VPNs)
   - Actions that cause unexpected alert by intrusion detection systems.
   - Unauthorized entry into the Data Center.

General requirements

In general, the security rule requires that health care organizations do the following:

- Make sure that information in computers is available when needed, that only people who should use it do so, and that it not be changed or corrupted by mistake.
- Protect patient information from any threats that the organization can anticipate.
- Guard against someone accidentally or intentionally giving out patient information to people who shouldn't have it.

As someone who works around patient health information, your role is to comply with all your organization’s policies to make sure that you don't create a situation where information is seen by someone who shouldn't have access to it, corrupted, or rendered unavailable.
But I already know this

Security is not a one-size-fits-all proposition. Since all health care organizations operate differently, your organization has conducted a risk analysis to develop policies and procedures that reflect its specific security needs.

Because each organization has its own risk areas, you will need to understand your organization’s approach to security. Even if you have received security training at other organizations, it's important to know the individual policies and procedures of the organization where you are working now.

Security awareness and the security officer

A security awareness training program is required by all health care facilities.

You will receive additional security reminders over time to re-enforce the initial training. Pay attention to these reminders to make sure you are always aware of your organization's latest security policies and procedures.

In addition, if you have questions about information security, be sure to bring them to your supervisor or your organization's information security officer. Your organization has chosen an individual to oversee information security and that person can answer any security-related questions.

The information security officer needs to know whether security policies and procedures are being violated or whether you notice something unusual that you think may represent a security problem. Contact them if you have any information security concerns.
YNHHS HIPAA Policy Summary: Information Security Incidents

YNHHS workforce members are required to report all information security incidents to the Information Security Officer or the MIS Help Desk (8-4357). All reported incidents will be investigated and the results reported to YNHHS management.

Key Points- Incident Examples
1. Using someone else’s ID or password.
2. Unauthorized transmission of protected health information (PHI) or confidential data over the Internet (for example, unencrypted transmission of a patient’s medications)
3. Introduction of a virus or worm into the computing system or network.
4. Unauthorized use of computing equipment by workforce or non-workforce members.

Everyone plays a role

The security officer has ultimate responsibility for the information security policies in place at your organization. However, everyone in the organization has an important role to play in keeping information secure by following policies and procedures.

Properly managing your password, preventing the spread of viruses, and ensuring proper disposal of materials that contain PHI are all important ways you contribute to information security.

Passwords

Choosing a strong password, or a password that is not easily guessed, is an essential step in securing the information in your organization. You probably will be asked to choose your own password in accordance with your organization’s policy.

If your organization does not have specific rules governing password selection, here are some good rules to apply as you select a password. Select something that is difficult to guess. Names of sports teams, personal names, and dates of birth are all passwords that are easily guessed. And software programs are readily available that can guess many common passwords, such as words or names. For that reason, you should choose a password that is made up of letters and numbers, at least six characters long, and incorporates both upper and lower case letters if your system supports this.

It’s not as hard as it sounds. One good way to do this is to create a password that represents something to you. For example, pick a subject you’re interested in, such as books, movies, sports, birds, or country music. Think of a related title or phrase. Select the first letter of each of the first four or more words. Insert two or more numbers and/or special characters. Now you have a good password that appears meaningless to everyone but you. For example if your subject is nursery rhymes, "Little Jack Horner sat in a corner" becomes with a few numbers inserted: L2Jh4s.
If you are unable to remember your password, write it down in a secure location that only you can access. Never put it in your desk or on your computer. And change it regularly, in accordance with your organization's policies. If your organization has no policy, a good rule of thumb is to change your password at least once every three months.

Even with sophisticated software, the most common way that a password is compromised is by its owner giving it out to someone. No one but you should know your password. If a coworker requests your password, refer that person to your organization’s help desk or tech support office so they can get appropriate access to the information they need. If you share your password—even if you think it is for a good reason—you are violating security policy.

Immediately report anyone outside the organization asking for your password, even if they say they are a vendor or help desk employee.

### YNHHS HIPAA Policy Summary: User Authentication to Computer Systems

YNHHS workforce members are provided with access to various computing systems which are needed in the performance of their jobs. Each user is authenticated by the use of an ID and password or other security mechanism.

**Key Points**

1. You may not share your password with anyone, for any reason.
2. Passwords are not to be stored on your computer or anywhere where they may be found by others.
3. Passwords should be at least 5 alphabetic and numeric characters in length.
4. You must report any unauthorized use of your password immediately.
Case Scenario #1: The Situation

You keep forgetting your new password, so you save it in a document on your desktop named "password."

Is this an acceptable practice?

Case Scenario #1: The Solution

No. You cannot keep your password where it is easily accessible. If someone finds your password and logs in to the facility's system as you, you can be held accountable for anything that happens because of it. If you have trouble coming up with a password, you can try the previous tips suggested or ask your information technology department or your information security officer for help coming up with a good password.

Physical security

While information security relies on technical measures, such as passwords, physical security also plays an important role. The following are some tips to ensure physical security:

- If someone inside the office wants to work on your computer, make sure to ask for identification to ensure that the person is a technical support employee of the facility. And always ask why he or she needs access to your computer.
- Do not remain logged-in to your computer when you are away from your work station.
- If you have a computer assigned specifically to you, follow your organization's policies with regard to turning it off if you are out.
- Your organization may have screen savers and keyboard locks that automatically engage when a computer is left idle. Do not attempt to defeat or disable these security devices.
- Practice common sense security. Make sure doors and desks are locked, as appropriate.
Case Scenario #2: The Situation

A worker from a department adjacent to you is using one of the computers in your area because their computer crashed. They insert a disk containing information about patients with HIV into the computer to pull up a list. They accidentally leave the disk in the computer and a temporary worker in your area sees the disk labeled “HIV Patients” and sells the information to a marketing company.

What should be done to prevent this type of problem?

Case Scenario #2: The Solution

Never leave a disk or anything containing patient information around for others to see or copy. Also, store all computer disks in locked areas and avoid labels that draw attention to file content. In this case, the worker using the computer in your area could have used a coding system for naming files and labeling disks that would not give away clues about the content.

Case Scenario #3: The Situation

You bring a laptop home to get some extra work done. You leave the laptop on the counter while you make dinner. Your daughter decides to use the computer without permission and accidentally e-mails patient information over the Internet to someone.

What should be done to avoid this?

Case Scenario #3: The Solution

When working from home the same precautions to protect information must be taken. Family members should not be using your work computer. If you leave your computer you should always exit out of your program or, better yet, log off the system and the network while you are away.

YNHHS HIPAA Policy Summary:
Safeguarding PHI and Confidential Information while Working Offsite

YNHHS policies and procedures regarding confidentiality are to be followed at all times when working offsite with PHI or other confidential information.
Case Scenario #4: The Situation

You receive a call from a man identifying himself as an IT worker at your facility. He starts asking you questions about your password and tells you there is a problem with your computer that he needs to fix. You did not request assistance from the IT department.

Should you give any information to this man?

Case Scenario #4: The Solution

No. Do not provide this man with your password. You should ask for his call-back number in your facility and call IT to confirm whether he is actually an employee, since an employee shouldn't ask for or need your password.
**Destruction of PHI**

When you "delete" a file from a computer disk or hard drive, you are not actually erasing it. When you click on "delete" or press the delete key, it's as though you were ripping the table of contents out of a book. Though they are hidden, the rest of the pages are still there and readable. The data in the file remains on the disk until it is overwritten. It's a relatively simple matter to recover those files that have not been overwritten.

For these reasons, your organization has special procedures for clearing disks or hard drives of all PHI and other data before they are allowed to be sold or reused. Some organizations will physically destroy drives, while others use special software to overwrite PHI until it can no longer be recovered. Never take a computer or disk from your organization for use elsewhere until it has been cleared by the department responsible for certifying that devices contain no PHI or other confidential data.

---

**YNHHS HIPAA Policy Summary:**

**Disposal and Control of Documents and Media Containing PHI**

YNHHS workforce members must ensure the protection of PHI by controlling the use, storage, and disposal of documents and other media-containing PHI.

**Key Points**

1. Types of media with PHI include, but are not limited to: Paper, Disks (including hard disks, floppy disks and compact disks), Microfiche, Overhead Transparencies, Photographs, Slides, Patient Identification Bands, I.V. Bags, Embosser Plates, Prescription Bottles.
2. When individuals have completed using PHI, media that contains PHI must be stored in a secure location, returned to the authorized owner, or the PHI or the media it is stored upon must be disposed of appropriately. Each type of media/document may require a specific disposal method for example, shredding confidential information.

---

**Computer hackers**

To secure information, you need to take certain precautions against threats that are unknown to you. Computer hackers-people who attempt to inappropriately access or disable computer networks-cause millions of dollars in damage each year.

As you've learned, the most common way they do this is by simply convincing someone to share a password or give them access by pretending to be someone they are not. However, there are technical ways that people can also access your network and you need to guard against these as well.
Viruses and other malicious software

A computer virus is a program or piece of computer code installed on your computer against your wishes. These programs can destroy information stored on your computer. They are often transmitted via e-mail attachments, and protecting against malicious software and viruses is an important responsibility. The following tips will help you guard against malicious software:

- Do not open any unknown attachments or unrecognizable e-mails.
- If you receive an unrecognizable or suspicious e-mail, immediately report it to your IT department or information security officer.
- Document and report any suspicious activity, such as unknown programs appearing on your computer.
- If you are provided with virus scanning software, always make use of it to scan e-mail or other files that you open on your computer.
- Don't use non approved e-mail. Web-based e-mail accounts, such as Hotmail, are convenient, but only use them if your technical support department approved of it.

YNHHS HIPAA Policy Summary: Computer Virus Protection

YNHHS facilities will ensure that current computer virus protection software is used on all electronic computing devices to protect PHI.

Key Points
1. Remote users or users of standalone devices must take reasonable steps to ensure adequate computer virus protection.
2. No member of the YNHHS workforce may intentionally remove or disable virus protection software installed on YNHHS-provided electronic computing devices.
3. If the current virus protection software reports the unsuccessful handling of a virus, or if users suspect the existence of a computer virus, they should immediately contact the Information Services’ Help Desk.
Case Scenario #5: The Situation

A doctor asks you to log onto her e-mail account to find and print an e-mail that she is expecting. She wants it ready for her review when she returns to the hospital.

*Should you do this?*

Case Scenario #5: The Solution

No. You should not have access to anyone’s e-mail but your own. The doctor should not give you her username and password.
Case Scenario #6: The Situation

You receive an e-mail from an unknown source that has an attachment. The e-mail reads that your computer has been infected with a virus and you need to follow the directions and open the attachment to get rid of it.

Should you follow the instructions?

Case Scenario #6: The Solution

No. Never open attachments from unknown sources. If you are unsure whether you should open something, contact your IT department for instructions.

Unauthorized software and hardware

Another source of security problems is software or hardware that is installed without the approval of your technical support department.

Music sharing software, remote access software, games, and other programs you may want to install can disable your computer or contain malicious software that would allow someone access to your computer. Don’t install any software on your computer without permission from your IT department.

Make a special note of the file extension at the end of a file name before opening it. You have probably seen file names that end with a ".doc." You should never open any files from an unknown source, but pay particular attention to files that end with a ".exe." These are executable files-software programs-and viruses or malicious software programs are often contained in downloaded executable files.

Use similar precautions when installing hardware. Any device attached to your organization's network needs to be installed with the appropriate security precautions in mind. For that reason, you should only connect other devices, such as computers or servers, to the network with permission from your technical support staff.
Case Scenario #7: The Situation

Your sister sends you an e-mail with a screensaver that she's says you would love.

*Should you download it on to your computer?*

Case Scenario #7: The Solution

No. Never put unapproved programs or software on your work computer. Your work computer is for work use only. Everything must be approved by your IT department.

E-mail use and transmission of electronic data

Information that is passed via e-mail is not usually secure. For that reason your organization has adopted strict policies with regard to how it electronically transmits PHI. Your organization's e-mail program may encrypt the information before sending it, or you may have special Web-based tools for transmitting patient information. Before you transmit patient information in electronic form, make sure you are in compliance with your organization's policies.
Encryption

Encryption simply means that the information is coded or scrambled so it cannot be read by anyone who doesn't have the key to read it.

Many organizations will encrypt the data they store or transmit depending upon whether there is a high risk that the information might be read by an unauthorized individual. Often this encryption process is carried out by software programs and operates invisibly to the user. You need to understand whether your organization requires you to encrypt data. Comply with that policy by using the approved tools for transmitting or storing patient information electronically.

Access control

One of the biggest changes under HIPAA involves access controls. In order to enforce security policies, organizations need to know who is accessing information and what information they are accessing.

In the past, many organizations allowed people to sign on under generic or shared passwords. But that practice is no longer allowed. Everyone should be assigned a personal user ID and password and should never use someone else's. Although it may be inconvenient at times, you must not let other people "borrow" your password to log on to the computer system. Similarly, you must not ask others to use their IDs and passwords.

In addition to creating a security problem, using someone else's access also may interfere with getting your job done. Your user ID and password are set up specifically for you to allow you access to the information you need for your job. Someone else's may not give you access to the information you need.

YNHHS HIPAA Policy Summary: Audit Controls

YNHHS facilities reserve the right to record and review audit trails of computer applications containing PHI and the operating systems they run on to ensure that data is only accessed and/or disclosed for treatment, payment and operations. Incidents of inappropriate access will be addressed by the Office of Privacy and Compliance and/or Information Security Officer.
Case Scenario #8: The Situation

A new worker in your area hasn't yet been given a username and password for the computer system. It is your responsibility to train them on the system.

should you just let them use your username and password until they have one of their own?

Case Scenario #8: The Solution

No. You should never allow anyone to use your username and password to log on to the system. In this case you should contact your supervisor or IT department to inquire as to when the new worker will receive their own username and password.

Case Scenario #9: The Situation

A patient comes up to your desk and demands to be removed from the patient directory. You do not have access to the directory, but since this patient is so upset, you decide to try and log in as a fellow worker by guessing his password. It works, so you take the patient out of the directory and log out. The patient is satisfied and calms down.

Is this a correct practice under HIPAA?

Case Scenario #9: The Solution

No. If you do not have access to the records as part of your job, you should not be accessing them. Even if the patient is upset and you know how to perform this function, you should never log in as someone else. Contact the appropriate person for the patient to assist them in having their name removed from the directory.
Log-in monitoring

Some organizations have computer programs that will alert users upon log-in of the date and time they last logged in. Take note of this information. If it is not correct, notify the information security officer.

For instance, if you arrive at work on a Monday after two days off, and you are notified that you last logged in on Sunday, that's a good sign that someone else is using your password and credentials to log in to the computer.

Also, if you have a computer that is assigned exclusively to you, take note if new programs are installed or you notice other changes; notify your information security office about the changes.

Working outside the organization

If you take information outside your organization, remember that many of the security precautions in place within the organization are no longer present at remote locations. Everything from security guards to virus checking software, to the watchful eyes of coworkers make up the information security infrastructure within your organization. When you take information outside the organization, you need to take additional precautions.

PDAs and laptops

Many health care workers, especially physicians, use personal digital assistants (PDA) and laptops. If you obtain a new wireless device that you want to use for PHI, contact the information security officer at your organization to ensure that it is acceptable.

The most frequent risk to using PDAs and laptops is the risk of theft of the device. PDAs should be locked in a drawer or briefcase when not in use, and if stolen, an incident report should be filed with your facility as soon as possible.

YNHHS HIPAA Policy Summary: Portable Electronic Devices

All members of the YNHHS workforce using portable electronic devices [e.g. laptops, mobile carts or PDAs], regardless of ownership, that store protected health information (PHI) must follow strict security standards since PHI can be inappropriately disclosed if the devices are stolen or accidentally lost.
Tips for using PDAs and laptops safely

The following are some helpful tips to help keep PHI secure while using a PDA:

- Never save PHI on a PDA unless it is password-protected
- Never keep passwords and access codes on your PDA under any circumstance
- Consider how data will be backed up, and work with your organization to ensure and protect backups
- Consider using encryption of sensitive data on your PDA and laptop

PDAs and viruses

Additionally, PDAs usually come with their own virus protection programs, but users often don’t enable or use those programs. If the organization's PHI will be used, transmitted to, or kept on a PDA, the user should make sure that virus protection is in place and up to date.

PDAs pose an additional problem with respect to viruses. Not only can PDAs be disabled by viruses, but other viruses that target computers can easily reside on a PDA without impacting the device, but then be transmitted to the organizations’ network during syncing and damage the network.

Conclusion

As you can see, information security is not the work of the IT department alone and is not guaranteed by technical safeguards of security software alone. It is the responsibility of all users of the information system to maintain security. As you go about your daily activities, remember the practices that make up the foundation of a strong information security program including:

- password management
- physical security
- awareness of changes to your computer
- protecting computers while you travel
- taking care with e-mail attachments
- adhering to your organization's policies

By focusing on these essentials, you will ensure that your organization's information remains secure and that you remain in compliance with the HIPAA security program.
DIRECTIONS: For each question below circle the best response among the choices listed.

1. True or false: It is allowable under HIPAA to log in to the facility’s system under a generic username and password.
   a) True  
   b) False

2. Which of the following is a common way to ensure physical security in the workplace?
   a) Make sure desk drawers and doors are locked, as appropriate.
   b) Verify the identification of anyone unknown requesting access to your computer.
   c) Never leave your computer on when you are gone for long periods of time.
   d) All of the above.

3. One of the requirements of the HIPAA Security Rule is:
   a) Convert all paper files to electronic documents.
   b) Protect against all reasonably anticipated threats or hazards to the security of protected health information.
   c) Limit the amount of visitors who can see a patient.
   d) None of the above.

4. Which of the following are ways to guard against computer viruses?
   a) Not opening unknown attachments.
   b) Documenting suspicious activity.
   c) Using virus scanning software.
   d) All of the above.

5. True or false: The most frequent risk to data security when using a PDA is theft.
   a) True  
   b) False

6. Software downloaded from the Internet, such as screen savers, music sharing programs, and games, can disable your computer or allow intruders to access data on our organization’s network.
   a) True  
   b) False
Confidentiality and Responsibility Agreement

I understand that as an employee, member of the medical staff, physician office employee, or non-YNHHS patient care provider or support personnel (volunteer, intern, student, contractor, vendor, etc.) of Bridgeport Hospital (BH), Greenwich Hospital (GH), Northeast Medical Group (NEMG), Yale-New Haven Hospital (YNHH) or Yale New Haven Health System (YNHHS), the performance of my job may require me to access or become aware of confidential information, such as:

- Patient health care and financial information (otherwise known under HIPAA as Protected Health Information or PHI)
- Employee personnel, compensation and health care information
- Physician performance and personnel information
- Business information relating to BH, GH, NEMG, YNHH, or YNHHS (including financial, administrative, resource management, and other information)

By signing below, I agree to the following:

a. I understand that approval to access and use this information in verbal, written, or electronic (stored in computer) form is a privilege. I also understand that access to delivery network or YNHHS information is granted to me based only on business or clinical "need to know" standards and the responsibilities of my job as an employee, member of the medical staff, or non-YNHHS patient care provider or support personnel. I agree to access information only on patients for whom I, my office, area, or department has responsibility. Patient information may be used for research or teaching purposes only when authorized by the appropriate institutional review board and in compliance with delivery network or YNHHS Policies and Procedures.

b. I understand that the methods I use to get information may only be used in the performance of my job. I understand that if granted a sign-on code, password, and/or "physical token device" that I accept full responsibility for any use or actions taken with my sign-on code(s), password(s) (codes), physical token device or Personal Identification Numbers (PIN), and recognize that, in some cases, these codes are the equivalent of my signature. The codes will be used only by me and I will not use another person's codes at any time. I will notify the IS "Help Desk" immediately should my code(s) be compromised in any way, or if my token is lost or stolen. I will reimburse the delivery network /YNHHS for the cost of the token, if not recovered. Violation of this Agreement will result in For Physicians: disciplinary action up to and including dismissal from the Medical Staff and/or House Staff of a member Hospital; For Employees: disciplinary actions under the guidelines of the delivery network /YNHHS Policies and Procedures; For Non-Employees: disciplinary actions up to and including immediate termination of your relationship with the relevant delivery network. In addition, violation of this Agreement may result in possible legal action, or fines against you and the organization you represent.

c. I understand that I may not seek access to any information that is not required to do my job. I understand that an audit trail, noting my code(s) or PINs, the patient, or system accessed and the date may be reviewed by the delivery network or YNHHS. I understand that patient information accessed through the computer is considered the same as the patient's medical record and may not under any circumstances be re-disclosed without proper authorization as covered in the YNHHS and/or Hospital By-Laws and Policies and Procedures. I agree to access, use, store and dispose of information which I use in a way that ensures continued security and confidentiality in accordance with delivery network /YNHHS Policies and Procedures.

d. I understand that computer hardware, software, and information are considered delivery network or YNHHS property and are subject to and protected by appropriate delivery network/YNHHS Policies and Procedures.

e. I understand that the delivery network /YNHHS reserves the right to make modifications to its access program including revoking codes and requesting the return of any token access devices.

f. I understand my access privileges will be revoked if any of the above understandings are violated.

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Print Name:</th>
<th>Title:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Affiliation: (i.e. BH, GH, HSC, NEMG, YNHH or Affiliate, Yale University, Community, Company, Other)</th>
<th>Dept.: (Dept., service)</th>
<th>MSO#: (If applicable)</th>
</tr>
</thead>
</table>

Last revised June 28 2016
Undergraduate Student Nursing Clinical Placement-Student Form

Student Name: ___________________________  Today’s Date: ___________________________

Affiliated School: ___________________________  Semester: ___________________________

Phone Number: ___________________________

Emergency Contact/Number: ___________________________

PLEASE REVIEW

RECORDS OF ITEMS BELOW ARE TO BE KEPT WITH SCHOOL COORDINATOR/DEPARTMENT

➢ I acknowledge I have completed the Connecticut Hospital Associate web-based “Health & Safety Training Course” Each student must successfully complete with a least an 85%

➢ I acknowledge I have received and reviewed the YNHH Nurse Orientation Program

➢ I acknowledge I have received and reviewed the YNHH Compliance, Privacy & Information Security documents

➢ I acknowledge I have received and reviewed the YNHH High Reliability Organization Program

➢ I acknowledge I have received and reviewed the YNHH Infant/Child Abduction Program
(Pediatrics/OB only)

➢ I acknowledge I have received and reviewed the YNHH Operating Room Program (OR only)

➢ I acknowledge that my AHA or ARC CPR certification is current

➢ I acknowledge I have a completed physical with all immunizations including: MMR, Varicella, Tdap, Hepatitis B, PPD (annual), Flu (annual), Tetanus (within 10 years)

➢ I agree I am in good health and capable of performing work assigned

➢ I acknowledge I will receive an EPIC login

By signing your name below, you are acknowledging that you have read and fully understand the information contained here.

Student Signature: ____________________________________________________________

PLEASE READ AND SIGN THE YNHH CONFIDENTIALITY AND RESPONSIBILITY AGREEMENT ALONG WITH THIS FORM AND RETURN TO SCHOOL COORDINATOR

REV. 1 (12/18)
Certification of Academic History

As a matriculating student to the 2019-2020 cohort of the CT Community College Nursing Program (CT-CCNP), I certify that I have provided true, correct, and complete information.

I acknowledge understanding that any misleading information provided by me in my application to the CT-CCNP or at any time thereafter may be cause for immediate dismissal from the CT-CCNP.

Name (please print): __________________________________________________________

Signature: __________________________________________________________________

Date: ____________________________

This form must be received at the following address by June 21, 2019:

Mary Beth Banks
Enrollment Services Assistant
Gateway Community College
20 Church Street
New Haven, CT 06510
Gateway Community College Non-Discrimination Notice

Gateway Community College is committed to equal access for persons with disabilities. Academic adjustments are provided to students with documented disabilities to assure access to academic and campus programs. For more information about academic adjustments and how to request them, please contact Ron Chomicz or Samantha Kusiak, Student Accessibility Services, Room S202, (203) 285-2231, rchomicz@gatewayct.edu; skusiak@gatewayct.edu. SAS works with students to discuss individual requests, review the type of adjustments and services that the College may provide and inform them about any documentation that may be necessary to arrange for certain adjustments. Students with disabilities are encouraged to contact the office at least one month before classes begin to avoid any delay in providing academic adjustments, especially when the College must arrange for external resources to provide the adjustments. Please also note that academic adjustments cannot be given retroactively.

For further information, please visit http://www.gatewayct.edu/Offices-Departments/Student-Accessibility-Services
Student Statement of Responsibility—Academic Adjustments

**Students with a Diagnosed Disability** must self-disclose and provide appropriate documentation to an Accessibility Specialist within Student Accessibility Services. This process must be done before services are provided. A request should be made every semester if the student requires reasonable academic adjustments. Services are not retroactive.

For more information contact Student Accessibility Services at 203-285-2231 or by email at rchomicz@gatewayct.edu; skusiak@gatewayct.edu. Student Accessibility Services is located in Room S202, second floor of the South Building.

Please see GCC Policy at [http://www.gatewayct.edu/Offices-Departments/Student-Accessibility-Services](http://www.gatewayct.edu/Offices-Departments/Student-Accessibility-Services)

I acknowledge that I have received written directions on the procedure for requesting academic adjustments, including when and to whom to make the request.

_____________________________  
Student Name (Please Print)

_____________________________  _________  
Student Signature  Date

This form must be received at the following address by June 21, 2019:

Mary Beth Banks  
Enrollment Services Assistant  
Gateway Community College  
20 Church Street  
New Haven, CT 06510
Required Textbooks and Digital Teaching & Learning Materials for Nursing Students

Pearson printed textbooks and digital teaching and learning materials will be provided through includED.

Access to digital materials is provided through Blackboard and students will pick up printed textbooks at their college bookstore.

Through includED the discounted cost of required textbooks and digital teaching and learning materials is part of the tuition and fees payment each semester of the nursing program. Students receive the Pearson materials that will be used throughout the entire program as they begin the first semester. As part of the includED program students pay for these materials in four equal installments of $247.75 when they register for each of the following courses:

- NUR*120 in the first semester,
- NUR*125: in the second semester,
- NUR*220: in the third semester, and
- NUR*225 in the fourth and final semester

An overview of these resources will be presented at the mandatory college nursing program orientation. A more detailed presentation by Pearson representatives and nursing faculty during the first day/week of classes will assist students to access and use the digital and printed learning resources effectively.

Students are encouraged to ask questions about the includED program at their mandatory college nursing program orientation. Students may also contact their college bookstore representatives with additional questions:

<table>
<thead>
<tr>
<th>College</th>
<th>Contact Person</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital</td>
<td>Loreen Wall</td>
<td><a href="mailto:0825mgr@follett.com">0825mgr@follett.com</a></td>
</tr>
<tr>
<td>Gateway</td>
<td>Pedro Rosenberg</td>
<td><a href="mailto:0809mgr@follett.com">0809mgr@follett.com</a></td>
</tr>
<tr>
<td>Naugatuck Valley</td>
<td>Joe Bocci</td>
<td><a href="mailto:1169mgr@follett.com">1169mgr@follett.com</a></td>
</tr>
<tr>
<td>Northwestern</td>
<td>Nancy Mueller</td>
<td><a href="mailto:0828mgr@follett.com">0828mgr@follett.com</a></td>
</tr>
<tr>
<td>Norwalk</td>
<td>Laury Thomas</td>
<td><a href="mailto:1168mgr@follett.com">1168mgr@follett.com</a></td>
</tr>
<tr>
<td>Three Rivers</td>
<td>Cheryl Pollard</td>
<td><a href="mailto:0807mgr@follett.com">0807mgr@follett.com</a></td>
</tr>
</tbody>
</table>
Please note: Per U.S. Department of Education federal regulation 34CFR688.164, students have the right to opt out of the includED program. However, it is important to note that opting out will:

- ELIMINATE access to all of the digital resources and learning activities embedded in the nursing courses
- ELIMINATE access to the purchasing discounts negotiated as part of the includED program
- ELIMINATE the ability to pay for textbooks and digital teaching materials in equal installments throughout the program
- REQUIRE students to pay the total retail cost of all required textbooks and digital teaching materials up front when they start the nursing program

The decision to opt out is final on the last day of the add/drop period each semester.

Refunds for the includED program are consistent with the college tuition refund schedule.

A student may obtain the includED opt out form from their Nursing Program Director following the mandatory orientation session.