INFORMATION SECURITY & CONFIDENTIALITY AGREEMENT

The information systems of Pennsylvania College of Health Sciences (PA College) are intended for the use of authorized members of the community in the conduct of their academic and administrative work. PA College's information systems consist of all networking, computing and telecommunications wiring, equipment, networks, security devices, passwords, servers, computer systems, computers, computer laboratory equipment, workstations, Internet connection(s), College-owned mobile communications devices and all other intermediary equipment, services and facilities. These assets are the property of the College.

Notwithstanding the right to audit or monitor its information systems, all users are required to observe the confidentiality and privacy of others' information accessed through PA College information systems and records of every description, including information pertaining to College programs, students, faculty, staff and affiliates. Without proper authorization, users are not permitted to retrieve or read content not intentionally addressed to them. With proper authorization, the contents of electronic mail or internet messages or materials may be accessed, monitored, read or disclosed to others within the College or otherwise.

Use of PA College information systems must comply with provisions of copyright law and fair use. Copyright law limits the rights of a user to decrypt, copy, edit, transmit or retransmit another's intellectual property, including written materials, images, sounds, music, and performances, even in an educational context, without permission, except where such use is in compliance with Fair Use or TEACH Act provisions.

Each individual granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Individuals are required to abide by all applicable Federal and State guidelines and PA College policies regarding confidentiality of data including:

- Access data for the sole purpose of performing his/her responsibilities.
- Not seek personal benefit or permit others to benefit personally from any data
- Not release College data other than what is required in completion of academic/job responsibilities.
- Not exhibit or divulge the contents of any record, file or information system to any person except as it is related to the completion of their academic/job responsibilities.
- All transactions, processed by a user ID and password, are the responsibility of the person to whom the user ID was assigned. The user's ID and password must remain confidential and must not be shared with anyone.
- Individuals are not permitted to operate or request others to operate any College data equipment for personal business, to make unauthorized copies of College software or related documentation or use such equipment for any reason not specifically required by the individual's academic/job responsibilities.

I understand that my access to College data and information is for the sole purpose of carrying out my academic/job responsibilities. Breach of confidentiality, including aiding, abetting, or acting in conspiracy with any other person to violate any part of this policy, may result in sanctions, civil or criminal prosecution and penalties, employment and/or College disciplinary action, and could lead to dismissal, suspension, or revocation of all access privileges. I understand that misuse of College data and information and any violation of this policy or the FERPA policy are grounds for disciplinary action, up to and including, dismissal.

It is the individual's responsibility to report immediately to his/her faculty/advisor/supervisor any violation of this policy or any other action, which violates confidentiality of data.

In addition to the Pennsylvania College of Health Sciences' information network you may also require access to computer systems within the Penn Medicine Lancaster General Health information network. By electronically agreeing to the terms and conditions of the College network you are also agreeing to the following Penn Medicine Lancaster General Health conditions.

Penn Medicine
Lancaster General Health

CONFIDENTIALITY AND ACCESS AGREEMENT

Lancaster General Health (LG Health) recognizes that you may have access to confidential information including, but not limited to, patient records (including patient demographic information), financial records, and personnel or other business-related information, either directly or indirectly (together, "Confidential Information"). All types of Confidential Information must be protected. As a condition to being granted access to Confidential Information, you agree to:

1. Only access Confidential Information on a need-to-know basis to perform your job duties or fulfill your contractual obligations.
2. Never access Confidential Information out of curiosity or non-business-related reasons. By way of example only, unless you have a business need to do so, you must not access records relating to the following:
    - Your immediate or extended family members (for example, your spouse or children),
    - Your friends, significant others, co-workers,
    - People in the news (for example, accident victims or famous people).

NOTE: Accessing <u>your own</u> electronic health record out of curiosity or for non-business-related reasons is outside the performance of your job duties and, therefore is **<u>prohibited</u>**.

- To request access to your own health record, contact Medical Records Services (717-544-5913).
- You can also access and manage your own records online through your own personal MyLGHealth account.

3. **Protect** Confidential Information by:
    - Logging off or locking the computer before you walk away from it
    - Encrypting any mobile device (for example, a smartphone, tablet, laptop, or USB drive) that has Confidential Information on it
    - No leaving Confidential Information or mobile devices containing Confidential Information unattended or within public access or view
    - Not leaving Confidential Information unattended or within public access/view – including paper, computers, mobile devices, etc.
    - Never share your password with anyone.
    - Immediately report confirmed or suspected privacy or security concerns or violations (see below for reporting methods).

Also, as a condition Information being granted access to any Confidential Information, you acknowledge and understand that:

- All forms of Confidential Information must be protected, including written, electronic, oral, overheard or observed. Patient information must be treated as confidential in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and any other state or federal law that may apply.
- You are prohibited from removing, retaining, disclosing, using or sharing Confidential Information after you are no longer working for or affiliated with LG Health.
- Your user ID and password is your electronic signature and is treated as your written signature with all legal implications.
- You are responsible for any action taken or documentation made when you are logged into a system or application with your user ID>
- Your access to LG Health systems and its content (for example email) may be checked from time to time by LG Health.
- If you do not comply with this Agreement, you will be subject to immediate corrective action, up to and including termination of your access to LG Health electronic systems and/or your employment or affiliation with LG Health, if applicable.
- If your access, employment and/or affiliation are terminated for violations of this Agreement, you may not be allowed access to LG Health information systems even if you become employed by another health care provider or company.

NOTE: All workforce members must follow all other LG Health policies and procedures relating to accessing electronic systems. LG Health workforce includes, but is not limited to, employees, medical staff, students, faculty, volunteers, temporary personnel, and other persons under the direction of LH Health, whether or not they are paid by LG Health.

To report information security or privacy violations or concerns to the Entity Privacy Officer you can email Privacy@LGHealth.org, call 717-544-4060, or call anonymously Compliance Alertline at 1-888-411-3380.

I have read the above and agree to comply with Pennsylvania College of Health Sciences' INFORMATION SECURITY & CONFIDENTIALITY AGREEMENT and Penn Medicine Lancaster General Health's CONFIDENTIALITY & ACCESS AGREEMENT as well as any updates or revisions published or posted.

3/2020