

Purpose: To preserve the privacy and confidentiality of all data and information handled by PA College, to define the rights of users and the rights of PA College to the handled data and information, and to define the practices implemented by PA College to handle the data and information.

Scope

This policy applies to the faculty, staff, and students of PA College of Health Sciences as well as trusted third parties and their representatives that work with the College.

Definitions

Data

Values without context. Used for reference and analytics.

Information

Data with context/meaning; processed data.

Access

Having the ability to read, edit, modify, and/or delete data and information.

Confidentiality

Keeping data and information private. This means that only accounts that have access to the specific data and information can see and work with it.

Integrity

Keeping data and information consistent and uncorrupted.

Availability

Having the data and information when it is needed.

Storage

Where data is accessed from. This can be local (i.e. the hard drive on a device) or in the cloud.

PA College system

Any device, application, cloud-based system, or other product that PA College owns or licenses.

Personally Identifiable Information (PII)

Information that can be identifies an individual on its own or can be used in combination to identify an individual uniquely.

- System credentials
- Social Security Number
- Other types of sensitive information (Health, Financial, Educational, etc.)

Directory Information

PA College has designated certain information in the education records of its students as directory information for the purposes of FERPA. The following is considered directory information at PA College:

- The student's name, address, email address, telephone number
- Day and month of birth
- Major field of study
- Participation in officially recognized activities and sports
- Dates of attendance, enrollment status
- Photographs
- Degrees and awards, and scholarships received
- Names of previously attended educational institutions

Authorized Individual

An individual allowed to make decisions on certain data/information. Typically, this is the owner of the data/information.

Release of information

Disclosure of personally identifiable information (PII) to any third party organization regardless of business affiliation.

Consent of release for PII

A confirmed approval of an authorized individual to collect, use, and potentially release that individual's personally identifiable information (PII) for reasons specified by PA College. This approval may be written, through an electronic form, or physical form. Individuals authorized to consent are typically owners of the data or information. Individuals who provide consent are declaring to have the authority to do so and are subject to non-compliance stipulations within this policy upon false testimony.

Privacy of Data and Information on PA College systems

Pennsylvania College of Health Sciences is an institution of higher education, dedicated to education, scholarship and the pursuit of knowledge. It is not the intent of this policy to impose restrictions that are contrary to PA College's established culture of openness, trust and integrity. However, the data and information that PA College operates with is critical to the continuity of its business and can be sensitive in nature. As part of a commitment to protecting PA College faculty, staff, students, and third parties working with PA College from illegal or damaging actions by individuals, either knowingly or unknowingly, it is the responsibility of everyone to know these guidelines, and to always maintain the confidentiality, integrity, availability, and legal compliance of data and information.

PA College is dedicated to protecting the overall privacy of all faculty, staff, students, and any other individual within the PA College system and those working with PA College. There is no expectation of privacy from PA College with any data or information that involves the usage of PA College systems. PA College may monitor any systems under its administration at any time, without notice or user

permission to maintain protections and the overall privacy of data and information residing on PA College systems.

Any personal data and information (meaning non-business or non-academic material) is subject to review when stored on a PA College system. Any users who store personal data and information on PA College accounts/systems accept sole responsibility for their own data and information. Reviews of accounts, data, and information will maintain a scope based on business need and will not go beyond what is deemed necessary in the scope of the review; however, there is a risk that personal data and information could be captured. It is in the best interest of any user of a PA College system to refrain from storing personal data and information (non-business or non-academic) on any PA College system to avoid any unintentional review or altering of personal data/information.

PA College employees and trusted parties will operate in good faith. College employees and trusted third parties are required to report the findings of potentially illegal data/information that is found whether intentional or unintentional.

Beyond having mitigations implemented, PA College will strive to remain transparent and forward while working with any data and information. When accessing or collecting any sort of data and information, access to the data and information and its use will be limited to only what is necessary for business need. Furthermore, PA College will disclose the purpose of collection and use of personally identifiable information (PII) and other sensitive data and information within this policy. PA College will only collect and use PII with proper consent, when needed, from the requestee and only through secure transmission procedures. Access to sensitive information outside the scope of normal business function will only be provided after justifying and approving the request through formal process and documentation of the request.

For transparency, employees will be notified of this policy upon hire. In addition to what is contained within this policy, students must refer to the *Educational Records Academic Policy* for how their educational records are handled by PA College.

Collection of Information

PA College will collect various forms of information for different reasons including but not limited to:

- Provision of services
- Business reporting and personalized services
- Aggregating personal information
- Business activity and operational purposes
- Other forms of data collected will be specified at the time of collection along with the purpose for collection

Third Party Payment Service

We will use third-party payment services to process payment cards when using certain services. If you wish to make a payment through the Services, your Personal Information will be collected by such third party and not by us, and will be subject to the third party's privacy policy, rather than this Privacy Policy. We have no control over, and are not responsible for, this third party's collection, use and disclosure of your Personal Information. This is to confirm with Payment Card Industry (PCI) standards and for the protection of your PCI information.

Consent to Collect, Use, and, Disclosure or Release Information

Any individual will be made aware of what the information is potentially used for as well as how the information will be used through this and other PA College policies. The individual maintains the right to make additional inquiries prior to providing information. An individual can agree to the terms and conditions provided when information is being collected and voluntarily provide the information requested. **Upon agreeing to the terms and conditions and voluntarily providing the information to PA College, you are consenting for PA College to collect, use, and potentially disclose or release that information for purposes included in PA College policies, statements, and listed within the terms and conditions.** PA College will respect the decision to either provide or not provide the information asked for; however, there are business processes and services that do require certain information in order to be completed. Without the information specifically requested, certain services cannot be provided. Therefore, any individual that does not provide the information required for that service cannot receive that service.

Disclosure and Release of Data and Information

PA College maintains the right to securely disclose and release data and information it collects for the following reasons:

- To conduct business within the Penn Medicine/Lancaster General Health organization or to its affiliates for purposes within this policy
- To third parties with a legitimate business relationship with PA College to facilitate services provided to PA College
- Legal and regulatory compliance and other obligations
- Business analytics/reporting, activities, and other operational purposes

The disclosure and release of sensitive data/information must have the consent of the individual unless PA College is legally obligated to provide the information or unless PA College is not obligated to gather consent as stated by regulation.

Directory information may be released at the discretion of the College and without the consent of the student unless the student informs the Office of the Registrar in writing that all such directory information about him or her is not to be made public without his or her consent.

Rights of the Owner and/or Subject of the Information

To the extent these rights are provided to you by applicable law, if you would like to request to review, correct, update, suppress, restrict or delete Personal Information that you have previously provided to PA College of Health Sciences, object to the processing of Personal Information or if you would like to request to receive an electronic copy of your Personal Information for purposes of transmitting it to another entity, please contact us via ITS Support Request. We will respond to your request consistent with applicable law. ITS Security and other necessary parties will work with the individual to address any data/information privacy concerns.

Access and Monitoring of Electronic Communications and Systems

PA College will only monitor/access electronic communications and systems without consent or notification of its users under justifiable business circumstances. The circumstances include:

- When there is a legal obligation or order to do so
- Standard administrative audits and business functions to maintain the confidentiality, integrity, and availability of PA College systems

PA College requires review and approval to access and/or monitor electronic communications and systems for the following circumstances:

- Business continuity (e.g. After employee termination, leave, or other unavailability reason)
- Internal audit or investigation into a potential legal or institutional violation
- Requests for release of PII or another type of sensitive information handled by PA College

NOTE: Data and Information classified as Level 3 or Level 4 per the *Security of Data and Information Standards* is considered sensitive in nature. If you are unsure of the level of sensitivity of the information, contact ITS Security.

The individual(s) or group from which the approval must come from is dependent on the situation and will be evaluated case by case. Approvals will come from an authorized party two levels up on the organization chart from the affected individual unless the affected individual is already a Vice President or the President of the College. In most cases, this will be a Department Lead or Vice President. There may also be situations where the owner of the account will be asked for approval such as when access to the owner's email from another user is requested.

Requests for accessing and monitoring electronic communications and systems are to be submitted through ITS Security via ITS Support Request. ITS Security can also be reached at 717-947-6103. Review and decisions on the request will be made after gathering all necessary approvals. The requestor will then coordinate with ITS in order to resolve the request. All requests are handled in accordance with all other relevant PA College Administrative and Academic policies.

Retention Period

Retention of information is aligned with the PA College Document Retention Policy.

Policy Compliance

- I. Compliance Measurement
 - a. The Department of Information Technology Services team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.
- II. Exceptions
 - a. Any exception to the policy must be approved by the PA College Department of Information Technology Services team in advance. An exception can be requested through the service request form and forwarded to the Data Governance committee.
- III. Non-Compliance
 - a. Where there is evidence of violation of this policy, PA College may restrict or prohibit the use of its information communication technology resources. Violations of this policy shall be treated in accordance with applicable College policies and procedures. When a potential violation is identified, the appropriate department head, Department of Information Technology Services, and any other PA College employees or agents as are deemed appropriate, are authorized to investigate and initiate action in accordance with PA College policy. Violations may result in suspension or termination of service(s). In addition, PA College may require restitution for any use of information systems that violates this policy. PA College may also provide evidence of possible illegal or criminal activity to law enforcement authorities.

References: Acceptable and Responsible Use Policy; Security of Data and Information Policy; Security of Data and Information Standards; Educational Records Academic Policy Statement; Document Retention Policy

Audience: All College
Effective Date: 3/28/19
Date Revised:
Date Reviewed: 3/28/19
Owner: AVP IT