Policy Name:	COVID-19 Privacy Statement		
Associated Form(s):	N/A	Policy Number:	2022-12
Reviewed:	Non-Academic Policy Review Committee	Approved:	August 12, 2022
Approval Authority:	President Timothy L. Hall	Adopted:	August 13, 2022
Responsible Executive(s):	General Counsel	Revised:	October 29, 2021 October 12, 2021 December 2020
Responsible Office(s):	Office of the General Counsel	Contact(s):	General Counsel or Assistant General Counsel

I. Introduction

The COVID-19 pandemic has required Mercy University to adapt and change in numerous ways, so as to continue to meet the needs of our students by continuing to provide a high quality, personalized and competitive education. Some of the ways in which the University has changed its daily operations in light of COVID-19 so as to ensure the utmost safety of our University community include, but are not limited to mandating proof of the COVID-19 vaccination for on-campus students, employees, certain visitors, contractors and vendors, offering testing for COVID-19 on campus, conducting contact tracing for positive COVID cases, and a greatly expanded use by students, faculty and staff of virtual platforms such as Zoom, Microsoft Teams, and Blackboard Collaborate. With these and the many other changes implemented, Mercy believes it is important to reiterate that it takes personal privacy of all its Community Members very seriously. While we have a *Privacy Policy* which deals with the transparent use of the University's webpage, this Statement is meant to inform the University community about other areas where we ensure confidential and private information about employees and students in light of the adaptions made by the University in the face of COVID-19.

II. COVID-19 Vaccination Status Privacy Notice

Mercy University is committed to protecting your personal information and being transparent about what information is held and how it is used. We understand your concerns about privacy and assure you that we take privacy matters seriously. Therefore, we are providing this Privacy Notice to explain how your personally identifiable information, is collected and used as it relates to proof of the COVID-19 vaccine. The information you provide will be used only as outlined in this Notice. If you have questions regarding this Privacy Notice, you may direct them to kbowes@mercy.edu.

By submitting information to us, you give your consent that all information that you submit, including your personally identifiable information (PII), may be processed as described herein. If you do not agree to be bound by this Privacy Notice, you may choose to not submit information to us.

A. Data We Collect. The information we collect is that which you provide to us, which will likely include, but not be limited to, the following:

- Full Name
- Telephone Number
- CWID
- Date of Birth (DOB)
- Date of First, Second Vaccine Doses (for Pfizer, Moderna, Novavax or other) or Single Dose (J&J/Janssen), and boosters (where applicable)
- Image of vaccination card or screen shot of Excelsior Pass.

B. Confidentiality and Storage

- This information will be kept confidential by the Student Health Office and the Office of Human Resources. It will be stored by the University in a safe and secure manner, in accordance with the Health Insurance Portability and Accountability Act (HIPAA).
- These records will be kept separate from employee/personnel and student records.
- Not providing the requested information may result in delays or restrictions in access to certain University programs and facilities that actively monitor immunity from the COVID-19 virus.

C. Information Usage

Generally, the University will use the information we collect through the COVID-19 Vaccination Status to assess the risk level of your full access to Mercy University facilities and programs. As this situation continues to evolve, we will follow the most up-to-date recommendations from the Centers for Disease Control (CDC) with regards to risks relating to COVID-19.

D. Information Sharing

We may share aggregate, non-personally identifiable information with other entities or organizations, including Mercy University or agents thereof, under the following circumstances:

- To assist in providing support for our internal operations.
- When legally required to do so, at the request of governmental authorities; to verify or enforce compliance with Mercy University policies, procedures and applicable laws; or to protect against misuse or unauthorized use of COVID-19 Vaccination Status.
- To measure utilization of the COVID-19 Vaccination Status by the Mercy University community, PII may be shared with the Mercy University Health Office under the following circumstances:
- To carry out their official duties in response to the public health crisis, including for case management and contact tracing purposes associated with public health orders.
- To assess whether individuals should be tested for COVID-19, and
- To provide individuals with information on medical care and consultation services specific to COVID-19.

III. Privacy Relating to Screening and Testing for COVID-19

A. Diagnostic Testing and Monitoring

Diagnostic testing and monitoring records are shared with the testing agency as well as Mercy University's Health and Wellness staff and State and County health officials. All testing records relating to a positive test are kept separate from any student or employee personnel

records, and are otherwise handled in accordance with what is permissible under the Health Insurance Portability and Accountability Act (HIPAA), where applicable.

B. Contact Tracing

Employees and students who test positive, or who have been exposed to someone in the University Community who tests positive, are expected to cooperate with the state or local department of health contact tracing efforts and to assist the University with its own internal contact tracing, if applicable. Any information shared (including cases in which an employee or student self-reports with the University) will be tracked separately from personnel records for employees and student records. The University will keep confidential the name of the infected employee or student to the greatest extent practicable.

Faculty and staff who learn of positive cases from students or employees (who report confirmed cases to them) are required to immediately inform the Director of Health and Wellness about these positive cases. Such employees who learn of positive cases and who are not involved in the University's official contract tracing program are not permitted to conduct their own investigation. Further, they are required to keep the information confidential to the greatest extent possible and unless required to disclose information pursuant to a request by the Director of Health and Wellness.

IV. Privacy Relating to Reasonable Accommodations Paperwork

All records relating to requests and granting of reasonable accommodations are kept in the Office of Human Resources (for employees) or the Office of ACCESSibility (for students). Such records are kept separate from personnel and student records and are shared only with those at the University outside of HR or ACCESSibiltiy when consent is granted by the employee or student, and on a need-to-know basis only.

V. Privacy Questions Relating to Zoom and Other Virtual Platforms

Questions have arisen from faculty, students and staff regarding use of video and recording over Zoom and other virtual platforms. For guidance about best practice for using Zoom and other virtual platforms, Mercy University Faculty should refer to the *Guidelines and Best Practices for the Use of Virtual Platforms in the Classroom* and students should refer to the *Virtual Etiquette* in the Student Handbook.

A. Use of Video

Faculty may require students to sign in with video while attending virtual classes, and staff supervisors may require employees to do the same. While Mercy does not have a specific "opt-out" option for using video-conferencing technology (e.g., Zoom, Blackboard Collaborate), students and employees who have privacy concerns for various reasons, including but not limited to child privacy concerns, domestic or interpersonal violence or other family concerns, or

homelessness, should contact their professor or the Office of ACCESSibility (for students); or their supervisor or Office of Human Resources (for employees).

B. Recordings

1. Notice. While there is no legal obligation under New York law to obtain your students' consent to record, it is required by some other states. As such, faculty must inform students (and other faculty and staff where applicable) in advance of recording and obtain their written consent (even if by email).
2. Opting out**.** Faculty should give students the ability to opt out of the recordings by turning off their cameras by muting their audio, not enabling video, and not typing into the Chat window. In these cases, students should still be considered in attendance and not penalized in any way.
3. Who is allowed to record? The faculty member, course staff and IT staff (upon request) are the only ones authorized to initiate a recording of a class. Further, faculty should make it clear to all students that they are not authorized to record a class, as per the Mercy Student Handbook.
4. Distribution of recordings**.** Faculty may only make recordings available to students in the class, and only through a password protected link on Blackboard. Faculty must make clear that students are not permitted to share the recording with anyone outside of the class pursuant to privacy laws, including the Family Education Rights and Privacy Act (FERPA).

Any privacy-related questions or concerns should be directed to the Department Chair (for students and faculty) or supervisor or manager (for staff). Any concerning incidents, such as unauthorized access and where threats or discriminatory remarks are made (such as Zoom-bombing) should be reported to the IT Help Desk as soon as practicable. And conduct that might be sexual harassment or other forms of discrimination should be reported to the Title IX Coordinator/Equity Compliance Specialist immediately.

VI. Privacy Relating to Telecommuting

With the increase in remote work, employees must adhere to the University's *Telecommuting Guidelines*. Employees are required to maintain confidentiality of employee and student records. In addition, employees are instructed that they should provide a secure location for University-owned equipment and materials, and will not use, or allow others to use, such equipment for purposes other than University business; and that the University is entitled to reasonable access to its equipment and materials.

VII. FERPA and COVID-19

The Family Educational Rights and Privacy Act (FERPA) affords eligible students rights with respect to their education records. One of the main protections under FERPA relates to the right to provide written consent before the University discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent as set forth in section III of the University's FERPA Policy. A number of questions have arisen in connection with COVID-19 and the protections afforded by FERPA. Many of those questions are addressed in the United States Department of Education's FAQs on FERPA and the Coronavirus, attached hereto.