# From Health to Identity :: Protecting You

## Office of the Registrar - Memorandum

8401 S. Chambers Road, Parker, CO 80134
(720) 874-2455 | registrar@rvu.edu

*This memorandum is a supplemental document to the FERPA Annual Notification, created by the Rocky Vista University - Office of the Registrar upon the outbreak of the coronavirus in early 2020 and updated for the Academic Year 2021-2022. The goal is to address the most urgent topics and FAQs expressed by the students, especially in light of its impact on record protection and the growing virtual environment of society. In this memorandum, you will find the headings:*

*A. Two-fold protection*
*B. What is allowed*
*C. Tips to protect your information*
*D. How FERPA applies to medical emergencies*
*E. Leader of the industry*

**A. TWO-FOLD PROTECTION:**

Contiguous with our efforts of protecting you physically in regards to health amidst this and any pandemic comes the equal and critical demand for protecting your identity, especially in regards to privacy of records amidst hybrid and remote situations. Now more than ever, with business also conducted virtually, I want to assure you that all RVU faculty and staff are trained and adhere to the FERPA guidelines. With the heightened use of internet-driven communication such as email, Teams, Zoom, document sharing, etc. we are all the more so taking measures to protect your information.

**B. WHAT IS ALLOWED:**

Remember, FERPA addresses various categories of matriculated student information, including but not limited to personally-identifiable information (PII), directory information, non-directory information, and education records. **FERPA does allow "school officials", including teachers, to access PII from education records provided they have "legitimate educational interest", i.e. a teacher's need to review an education record to fulfill their professional responsibility.**

**C. TIPS TO PROTECT YOUR INFORMATION:**

Even if we are cautious in handling your personally identifiable and academic information from our end, your identity can still be at risk if you allow your information to be exposed without your consent, with other students, to outside agencies, and of course to the open public. Therefore, below are a "top 5" I've narrowed down to help you protect your information, which should already be practiced on and off campus anyway:

1. **Observe a "clean-desk" policy**: your information should not be left accessible on your desk or study space when you leave for an extended period of time. If your study space is a publicly exposed area such as to classmates, roommates, your dining table, a den, etc., it is recommended to conceal your information away in a drawer or file.

2. **Lock your computer**: the computer is our electronic desk (it literally has a "Desktop") and therefore should be treated that way, in light of the clean-desk policy. Lock your computer (e.g. Windows key + L) every time you step away to prevent even the accidental public misuse or abuse of information. Computers have saved passwords, active log-ins, and open documents that should not be subjected to the wrong hands.

3. **Avoid haphazard communication**: be extra careful with online methods of communication and 3rd-party vendors and subscriptions, proof-read or re-read information in circulation, and think twice in your actions with technology. **Avoid the accidental Reply-All or forwarding of entire email chains**. Double-check when sharing your screen on Skype, Zoom, Teams or any other virtual platform. We are using new methods of technology and should be sure of what and how we are using it before actually using it.

4. **Guard the exchange of information**: there are various ways to protect the sharing of information, including password-protecting files that you are emailing, document-sharing or otherwise distributing, or encrypting an email.

5. **Protect each other**: as we look out for you, look out for each other. If you notice your peer or colleague is exposing their information in an unsafe way or not practicing the above tips, do them a favor and let them know. In this lifestyle where time escapes us and new habits are formed, it is easy to overlook these situations and therefore all the more helpful to keep each other accountable.

**D. HOW FERPA APPLIES TO MEDICAL EMERGENCIES:**

Attached is a FERPA & Coronavirus Disease FAQ document that was provided by the U.S. Department of Education for your reference upon the initial outbreak, outlining the applicability of FERPA to disclosures of student information related to medical emergencies. With the world still dealing with variants and spikes, the CDC still updating guidelines and requirements, and organizations still assessing the best methods of safety, this information still applies to current and upcoming circumstances. I encourage you to review on your own, but in the meantime, below are the overall points:

1. **Prior consent**: in general, students must provide written consent before an institution can disclose personally identifiable information (PII) from the student's education record to external parties or other students. To ensure protection, such information is disclosed by the Registrar's Office unless otherwise specified or an exception applies.

2. **Emergency exception**: an institution can disclose PII without prior consent if knowledge of that information is necessary **to protect the health or safety of others, but only during the time of emergency, such as now.** However, PII such as directory information is not disclosed in combination with non-directory information, such as health status or treatment.

3. **Appropriate parties**: the above exception applies to the disclosure of PII to "appropriate parties" such as public health and law enforcement officials. Under no circumstance can an institution without prior consent disclose PII to the media, even if the purpose is for alerting the community.

4. **Record-keeping**: in the rare cases of emergency exceptions, each instance of nonconsensual disclosure of PII from student education records is recorded, even if disclosed to public health or law enforcement officials, and even if to protect the health or safety of others during the time of emergency. Disclosures backed by prior consent are not required to be recorded.

**E. LEADER OF THE INDUSTRY:**

As a final note of assurance to you, I participated on a Colorado Department of Higher Education Council for COVID back in 2020, and upon interaction with other institutions, am proud to tell you that RVU is indeed a leader of the industry, in thorough action and response to medical emergencies, in serving and supporting you our students, and in ensuring your complete education and graduation for you to succeed in your careers, even amidst the pandemic and evolving society.

If you're still unsure about your rights or how to handle your information, consult your Registrar or Compliance Specialist, and we can help you determine the best course of action or point you in the right direction. Like with law enforcement, it is our job to protect you, but you must also keep yourself well-informed and do your part to stay protected.

Sincerely,
Your Registrar

David Paltza, MS
Office of the Registrar
Rocky Vista University