Emailing Sensitive University Information - What to Know

July 16, 2020 by Janet Bravo, OIS

As a member of the CU community, you play a vital role in safekeeping sensitive university information. If you have been entrusted to handle personally identifiable information (PII) or sensitive university information due to the nature of your job, you must be mindful of your responsibility to safeguard it from unauthorized access or accidental disclosure.

Email is an essential communication tool; however, there are risks when using it to share sensitive information. One such risk is sending sensitive content to unintended recipients in the body of email or as an attachment. The consequences of misdirected emails may include damage to our constituents’ privacy, as well as the university’s reputation and funding.

**Email Security Tips**

Take precautions to avoid accidental exposure of personally identifiable information (PII) or sensitive university information when sharing through email:

- Be mindful when using “Replying All” as it may include individuals who do not have a business need-to-know.
- Be careful with email auto-complete, a feature that automatically completes a name for you when you begin typing it in the TO field. It may enter the wrong name. Check the TO field a second time before sending the email.
- Consider the risk with forwarding information from your work to home email account; it’s not a best practice.
- Know that the "Recall This Message" is often not effective. This feature will only work if the message is still unread and you are sending to another person on your campus (excluding Boulder students and other Gmail users).
- Password protect attachments.
- Consult with your campus IT department about other options for sending sensitive university information, especially when it relates to HIPAA.

If you send an email containing sensitive university information to an unintended recipient, immediately notify the appropriate campus contact with information regarding who was sent the email and the type of information that was shared. See Report an Incident for additional details.

**What is sensitive university information?**

Know the type of information you handle, as that determines how to best keep it safe. Some examples include:
• Protected health information
• Social security numbers
• Payment card numbers
• Health insurance policy ID numbers
• Student information and admission applications
• Faculty and staff personnel records, benefits, salaries, ID numbers, and employment applications
• Donor contact information and non-public gift amounts
• Non-public policies
• Internal memos and email, and non-public reports
• Purchase requisitions, cash records, budgetary plans

See About Data Classification [4] for an expanded list.

Ensure you only have access to the information you need to perform your job. Talk with your supervisor if you’re not sure.

Display Title:
Emailing Sensitive University Information - What to Know
Send email when Published:
No

Source URL: https://www.cu.edu/blog/ois-blog/emailing-sensitive-university-information-what-know

Links
[1] https://www.cu.edu/blog/ois-blog/emailing-sensitive-university-information-what-know
[4] https://cu.edu/node/242757