

**Administrative Standard**

**Title: OIT FormStack Guidance**

Source: Office of Information Technology

Prepared by: OIT Risk and Compliance

Approved by: Sean Clark, Information Security Director,
Office of Information Technology (OIT)

Effective Date: April 6, 2018

Applies: This guidance applies to all users that access FormStack, which is managed by the CU Denver | Anschutz Medical Campus Office of Information Technology.

1. **Introduction**

Per University Policy, it is important that the confidentiality, integrity, and availability of Confidential and Highly Confidential data collected via FormStack is preserved.

1. **Guidance**

To maintain the security of University Confidential and Highly Confidential data, please ensure you are following the guidance below:

1. Do not send or do not include sensitive data in confirmation (to the submitter) emails
2. Encrypt and set a password on the submission database, only share the password with those who have a business need to see that data
3. Use HTTPS forms only
4. Do not allow attachment of files which contain sensitive data within forms
5. Do not enable integrations which use unencrypted data transfer

The confidentiality, integrity, and availability of University Confidential and Highly Confidential data depends on all of us. For more information regarding University HIPAA requirements, and University Policies with University Confidential and Highly Confidential data, please review the following links:

* [Data Classification & Impact](https://www.cu.edu/ois/data-classifications-impact)
* [University HIPAA Policy](http://www.ucdenver.edu/research/ORC/HIPAA/Pages/Policy.aspx)
* [University Policy APS-6005](https://www.cu.edu/ope/aps/6005)

If you have any questions regarding this service, please contact the CU Denver | Anschutz Medical Campus OIT Service Desk at 303- 724-4357.

**C. Review**

This standard will be reviewed no less than once every five years. However, threat vectors in Information Technology can evolve at a rapid pace creating new and unanticipated risks. As risks shift, this standard may be reviewed at any time at the discretion of the OIT Information Security Officer.