Which data should I not store in Quick Base?

Q: Which data should I not store in Quick Base?

Answer

Quick Base is not appropriate for all kinds of data.

The following categories of legally-protected data are inappropriate for storage in Quick Base

- HIPAA-protected data or other personally identifiable health information
- Data subject to United States export control or trade embargo regulations
- Social Security numbers, driver's license or other state ID card numbers, and financial account, credit card, or debit card numbers

If you are unsure if you are handling legally-protected data, please contact IS&T at infoprotect@mit.edu for assistance.

Best Practices for securing sensitive data stored in Quick Base

The following categories of legally-protected and sensitive data are appropriate for storage on Quick Base, provided that you take reasonable steps to secure the data in your Quick Base account:

- Student information
- Confidential information about employees
- Information about human research subjects
- Data received subject to access and use restrictions under a Data Use Agreement or Nondisclosure Agreement
- Other information of a confidential or sensitive nature

Such data should be reasonably secured by sharing only with persons who need to access the data for a permissible purpose, and under strict instructions that these persons (a) may not share the data with any third party, absent permission from you, and (b) should delete the data from their local systems when they are finished with it.

Devices used to access such data should be appropriately protected. Please review IS&T guidelines for device encryption and Encrypting a file before sharing for guidance.

General usage guidelines

When using Quick Base, you should always:

- Comply with MIT's policies, including those relating to Responsible Use of IT Resources.
- Remember the "analog hole": once data has been converted to a human readable form, there is no way to truly protect it. For example, even a PDF file with printing, saving, and copying restrictions can still be copied if the recipient uses a screen-capture tool, takes a picture with a mobile phone, or even copies the document longhand onto a piece of paper. Therefore, you should only share data with those you trust, and with only the minimum number of people necessary.