

Interoperability and Spectrum Health

In alignment with the 21st Century Cures Act (the Cures Act), Spectrum Health patients are now able to access their electronic health data in applications (apps) of their choosing (not only the MyChart patient portal). The goal of the Cures Act is to give patients greater control over their health information. Click [here](#) for additional information on what interoperability means for you as a patient.

At this time, the Cures Act only requires Spectrum Health to share a specific subset of your electronic health information (EHI). Click [here](#) to learn more about the USCDI V1 data set. Many of these items were already shared with you through MyChart. Spectrum Health also now provides you the ability to share your EHI with apps. You can request that your health information be shared directly with an app of your choosing if the app is set up to connect with Spectrum Health.

Spectrum Health encourages greater access to electronic health data while still urging patients to think about the privacy and security considerations noted below prior to providing a third-party app access to EHI. Below are some steps you may take to protect your privacy and security as related to apps.

Steps You May Take to Protect Your Privacy and Security

- **Review the App's Privacy Policy and/or Terms of Service:** It is important that you understand the security and privacy practices of any app that you entrust your health information. You should feel comfortable asking whether the app has a Privacy Policy and/or Terms of Service. In some instances, the app's privacy and security language may be in the app's Terms of Service and not a separate Privacy Policy. If the app does not have a Privacy Policy, patients should evaluate the possible risks in moving forward with the app. Patients can consider the questions noted below when reviewing the Privacy Policy. If the app's Privacy Policy does not clearly answer the below questions, patients should reconsider using the app to access their health information. Health information is very sensitive, and you should be careful to choose apps with strong privacy and security standards to protect it.

Some questions you may want to ask or factors you should consider are:

- What health data will be collected?
- Will non-health data be collected from my device (ex: my location or any Internet search information)?
- Will my data be stored in a deidentified or anonymized form (ex: someone would not know the data was about me)?
- Will my data be stored or accessed outside the United States?
- How will the app use my data?
- What are the secondary uses of my data?
- Will my data be disclosed to third parties (other companies) by the app for any purposes (ex: research and advertisement)?
- Will this app sell my data to third parties for any reason?
- Will this app share my data for any reason? If so, with whom and for what purpose?
- How can I limit this app's use, disclosure, or sale of my data?

- What security measures will be used to protect my data?
 - How will I be notified if there are any security concerns or any data breaches?
 - What impact could sharing my data with this app have on others, such as my family members?
 - How can I access my data and correct inaccuracies in the data retrieved by this app? (Note that correcting inaccuracies in data collected by the app will not affect inaccuracies in the source of the data.)
 - Does this app have a process for collecting and responding to user complaints?
 - Does this app allow its customers to see user complaints and how they were resolved? Or does this app provide a question-and-answer forum?
 - How do I terminate the app's access to my data if I no longer want to use the app or if I no longer want this app to have access to my health information? How difficult will it be to terminate access?
 - What is the app's policy for deleting my data from the company's records once I terminate access? Is it more than just deleting the app from my device?
 - How will this app inform me of changes in its privacy practices?
- **Learn and Know Your Rights Under HIPAA and Who Must Follow HIPAA**
- The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification rules along with the Patient Safety Act and Rule. The HIPAA Privacy Rule covers health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically. Spectrum Health and the MyChart patient portal are all subject to HIPAA.
 - Click [here](#) to find more information about rights under HIPAA and who is obligated to follow HIPAA.
 - You may also want to click [here](#) for HIPAA FAQs for Individuals.
- **Determine if the Third-Party App is Subject to HIPAA:** Most apps will not be covered by HIPAA because they are not affiliated with entities governed by the HIPAA Privacy Rule. Apps likely fall under the Federal Trade Commission (FTC)'s jurisdiction and the protections provided by the FTC Act. Among other things, the FTC Act protects against deceptive acts (e.g., if an app shares personal data without permission, despite having a privacy policy stating that it will not do so). Click [here](#) for more information from the FTC about mobile app privacy and security.
- **Learn What You Need to Do if You Think Your Data Has Been Breached**
- You should keep in mind that once health information leaves Spectrum Health that there is a potential that the information released may be disclosed (released/shared) by the recipient (the app) and that it may no longer be protected by HIPAA.
 - The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule.
 - The Federal Trade Commission (FTC) (through the FTC ACT) protects against deceptive acts (e.g., if an app shares personal data without permission, despite having a privacy policy that says it will not do so). The FTC provides information about mobile app privacy and security for consumers if you click [here](#).
 - Therefore, if you believe your data has been used inappropriately or breached, you can submit complaints to the OCR by clicking [here](#) or to the FTC by clicking [here](#). The option you select depends on whether the app is subject to HIPAA.

- **Reach out to the Spectrum Health Privacy Team with Questions:** The Spectrum Health Privacy team can be reached at Privacy @spectrumhealth.org or via the Privacy Hotline at 1-616-486-4113.

- Visit these helpful websites found via the links below
 - [Who must comply with HIPAA privacy standards](#)
 - [What ONC's Cures Act Final Rule Means for Patients](#)
 - [ONC's Cures Act Final Rule](#)
 - [USCDI v1 Dataset](#)
 - [How to submit complaints to OCR](#)
 - [How to submit complaints to FTC](#)

As changes in federal regulations occur related to the Cures Act, this document will be updated accordingly.