



Interoperability & Protecting your Health Information

The Centers for Medicare & Medicaid Services (CMS) published the Interoperability and Patient Access Final Rule on May 1, 2020. This final rule focuses on driving interoperability and patient access to health information, by putting patients first, giving them access to their health information when they need it most and, in a way, they can use it best.

This regulation includes policies which require or encourage payers, such as Amida Care, to implement Application Programming Interfaces (APIs) to improve the electronic exchange of healthcare data—sharing information with patients or exchanging information between a payer and a provider or between two payers.

This rule gives patients access and use of their complete electronic health record (EHR), confidence that their health care providers are communicating and coordinating their care, and the ability to engage in their own care in a more meaningful way.

What does this all mean? It means, that, **with your consent**, Amida Care could share your health records with third-party applications (apps), to make the exchange of your health information more accessible to yourself, your providers and health insurers. Amida Care **will only share your electronic health information** with a third-party app developer **if you ask us to.**

Once you give Amida Care permission to share your electronic health information with a third-party app, it is important that you know that Amida Care is **no longer responsible** for the data once the app receives it. This means that Amida Care is not responsible for how the app uses your data or secures your data. This also means that once you give your consent to release your electronic health record to a third party app, the information received by the app may no longer be covered under the Health Insurance Portability and Accountability Act (HIPAA), because most third party app developers are not considered a “covered entity” under HIPAA. To find out more about HIPAA and who is required to follow HIPAA, **click [here.](#)** To see the **HIPAA FAQ**, **click [here.](#)**

It is important that you **carefully read any privacy and security notices issued by the app before consenting for Amida Care to release your electronic health information to an app.** An app developer should also disclose how it shares

Interoperability & Protecting your Health Information

sensitive information in their product documentation, according to the Federal Trade Commission (FTC).

Are third-party apps covered by HIPAA?

Most third-party apps will not be covered by HIPAA. Most third-party apps will instead fall under the jurisdiction of the FTC and the protections provided by the FTC Act. The FTC Act, among other things, 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 [here](#).

What are important things you should consider before authorizing a third-party app to retrieve your health care data?

It is important for you to **take an active role in protecting your health information**, and you should be careful to **choose apps with strong privacy and security standards**. If an app does not have a privacy policy, the Centers for Medicare & Medicaid Services (CMS) advises that you not use it. The app's privacy policy should clearly answer the below questions:

- What health data will this app collect? Will this app collect non-health data from my device, such as my location?
- Will my data be stored in a de-identified or anonymized form?
- How will this app use my data?
- Will this app disclose or sell my data to third parties?
 - Will this app sell my data for any reason, such as advertising or research?
 - Will this app share my data for any reason? If so, with whom? For what purpose?
- How can I limit this app's use and disclosure of my data?
- What security measures does this app use to protect my data?
- 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 data retrieved by this app?

Interoperability & Protecting your Health Information

- Does this app have a process for collecting and responding to user complaints?
- If I no longer want to use this app, or if I no longer want this app to have access to my health information, how do I terminate the app's access to my data?
 - What is the app's policy for deleting my data once I terminate access? Do I have to do more than just delete the app from my device?
- How does this app inform users of changes that could affect its privacy practices?

If the app's privacy policy does not clearly answer these questions, CMS says you should reconsider using the app to access your health information. **Health information is very sensitive information, and you should be careful to choose apps with strong privacy and security standards to protect it.**

What should a patient do if they think their data have been breached or an app has used their data inappropriately?

To learn more about filing a complaint with OCR under HIPAA, visit:
<https://www.hhs.gov/hipaa/filing-a-complaint/index.html>

Individuals can file a complaint with OCR using the OCR complaint portal:
<https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>

Individuals can file a complaint with the FTC using the FTC complaint assistant:
<https://reportfraud.ftc.gov/#/>

To learn more about Amida Care's Privacy Practices and how to contact us visit:
<https://www.amidacareny.org/wp-content/uploads/ac-notice-V4.pdf>