Client Privacy and Security Resources: Supporting Payers Educating Their Clients

On May 1, 2020, the Centers for Medicare and Medicaid Services (CMS) made a new rule called the **Interoperability and Patient Access Rule**. This rule helps you get easier access to your health information in a safe and secure way.

Who this rule applies to:

Most health insurance companies that work with CMS need to follow this rule. This includes:

- Medicare Advantage (MA) plans
- Medicaid Fee-For-Service (FFS) programs
- Children's Health Insurance Program (CHIP) FFS programs
- Medicaid and CHIP managed care plans
- Insurance companies offering Qualified Health Plans (QHPs) on the federal marketplace (Healthcare.gov)

Who is not included:

This does not apply to companies that only offer stand-alone dental plans or those offering QHPs for small businesses.

What the rule requires:

These insurance companies must:

1. **Create a secure system** (called an API) that lets you use a phone app or website to see your health records.
2. Use a specific technology standard called **HL7 FHIR Release 4.0.1** so all systems can work together.
3. Let you view your:
    - Past doctor visits (encounters)
    - Bills and how much you had to pay
    - What your insurance paid
    - Certain medical records
4. Allow you to use the app or tool *you* choose to view this information.
5. Give you helpful information about **privacy and how to keep your health data safe**.

Why this document exists:

When CMS created this rule, they asked for feedback. People said they wanted examples to help insurance companies create easy-to-understand resources for patients.

This document gives ideas of what those resources could include. Insurance companies don't have to use this document, but it's here to help them create tools that are clear, helpful, and right for the people they serve.

Helpful Information for Payers Creating Educational Resources for their Clients

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

It is important for clients to take an active role in protecting their health information. Helping clients know what to look for when choosing an app can help clients make more informed decisions. Clients should look for an easy-to-read privacy policy that clearly explains how the app will use their data. If an app does not have a privacy policy, clients should be advised not to use the app.

Clients should consider:

- 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 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?
- 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, clients should reconsider using the app to access their health information. Health information is very sensitive information, and clients should be careful to choose apps with strong privacy and security standards to protect it.

What should a client consider if they are part of an enrollment group?

Some clients, particularly clients who are covered by Qualified Health Plans (QHPs) on the Federally-facilitated Exchanges (FFEs), may be part of an enrollment group where they share the same health plan as multiple members of their tax household. Often, the primary policy

holder and other members, can access information for all members of an enrollment group unless a specific request is made to restrict access to member data. Clients should be informed about how their data will be accessed and used if they are part of an enrollment group based on the enrollment group policies of their specific health plan in their specific state. Clients who share a tax household but who do not want to share an enrollment group have the option of enrolling individual household members into separate enrollment groups, even while applying for Exchange coverage and financial assistance on the same application; however, this may result in higher premiums for the household and some members, (i.e. dependent minors, may not be able to enroll in all QHPs in a service area if enrolling in their own enrollment group) and in higher total out-of-pocket expenses if each member has to meet a separate annual limitation on cost sharing (i.e., Maximum Out-of-Pocket (MOOP)).

What are a client's rights under the Health Insurance Portability and Accountability Act (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, and the Client Safety Act and Rule. You can find more information about client rights under HIPAA and who is obligated to follow HIPAA here: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for- consumers/index.html

You may also want to share with clients the HIPAA FAQs for Individuals: https://www.hhs.gov/hipaa/for-individuals/faq/index.html

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 Federal Trade Commission (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: https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps

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

Payers should clearly explain to clients what their policy is for filing a complaint with their internal privacy office. In addition, payers should provide information about submitting a complaint to OCR or FTC, as appropriate. To learn more, see the resources below.

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://www.ftccomplaintassistant.gov/#crnt&panel1-1