Patient Privacy and Security Resources – Supporting Payers Educating their Patients

The Centers for Medicare and Medicaid Services (CMS) released the Interoperability and Patient Access final rule on May 1, 2020. This final rule requires most CMS-regulated payers – specifically, Medicare Advantage (MA) organizations, Medicaid Fee-For-Service (FFS) programs, CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on the Federally-facilitated Exchanges (FFEs), excluding issuers offering only Stand-alone dental plans (SADPs) and QHP issuers offering coverage in the Federally-facilitated Small Business Health Options Program (FF-SHOP) - to implement and maintain a secure, standards-based **Patient Access Application Programming Interface (API)** (using Health Level 7® (HL7®) Fast Healthcare Interoperability Resources® (FHIR®) Release 4.0.1) that allows patients to easily access their claims and encounter information including cost, specifically provider remittances and enrollee cost-sharing, as well as a defined sub-set of their clinical information through third-party applications of their choice. This rule also requires these payers to make resources regarding privacy and security available to all patients.

In the CMS Interoperability and Patient Access proposed rule, we asked stakeholders what kinds of information we could make available to help payers meet these requirements. Commenters asked us to provide sample information they could consult when producing their patient resource materials.

This document provides an overview of what is required to be included in a payer's patient resource document and some content payers may choose to use to help meet this requirement. Use of this document is not required; this is meant to support payers as they produce patient resources tailored to their patient population.

What the Rule Requires

The final rule requires impacted payers to provide in an easily accessible location on their public websites, or through other channels used for regular communication with patients, educational resources in non-technical, simple, and easy-to-understand language that explains, at a minimum:

- General information on steps the individual may consider taking to help protect the privacy and security of their health information, including factors to consider in selecting an application including secondary uses of data, and the importance of understanding the security and privacy practices of any application to which they

will entrust their health information; and

- An overview of which types of organizations or individuals are and are not likely to be Health Insurance Portability and Accountability Act (HIPAA) covered entities, the oversight responsibilities of the Office for Civil Rights (OCR) and the Federal Trade Commission (FTC), and how to submit a complaint to OCR and the FTC.

The CMS Interoperability and Patient Access final rule also encourages impacted payers to ask third-party app developers to attest to having certain provisions in their privacy policy. Payers that ask for this attestation should share with the patient a clear explanation of what the attestation is asking and how the process will work as part of their educational resources. It is important to make sure patients understand that if an app developer is asked to attest and does not respond to this request or attests negatively, the patient will have an opportunity to change their mind about sharing their data. But, if the patient does not actively respond to the payer within the period of time clearly communicated to them by the payer, the patient's data will be shared as they originally requested.

Helpful Information for Payers Creating Educational Resources for their Patients

<u>What are important things patients should consider before authorizing a third-party app to retrieve their health care data?</u>

It is important for patients to take an active role in protecting their health information. Helping patients know what to look for when choosing an app can help patients make more informed decisions. Patients 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, patients should be advised not to use the app. Patients 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, patients should reconsider using the app to access their health information. Health information is very sensitive information, and patients should be careful to choose apps with strong privacy and security standards to protect it.

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

Some patients, particularly patients who are covered by QHPs on the 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. Patients 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. Patients 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 patient's rights under HIPAA and who must follow HIPAA?

The U.S. Department of Health and Human Services (HHS) OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule. You can find more information about patient 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 patients 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 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 patient do if they think their data have been breached or an app has used their data inappropriately?

Payers should clearly explain to patients 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 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/#/