Final July 30, 2025

Real-Time Claims Processing Pilot and Opportunities to Enhance Medicare's Electronic Data Interchange (EDI) Cybersecurity Controls Listening Session

As part of the Centers for Medicare & Medicaid Services (CMS) 2025 priorities, we are holding a listening session to gather feedback from our industry partners to gather innovative ideas and opportunities for real-time claims processing. We are also looking to improve Medicare's Electronic Data Interchange (EDI) cybersecurity controls which support the security and integrity of electronic transactions physicians, suppliers and other providers use to submit Medicare Part A and Part B claims.

We invite you to participate in the CMS Listening Session scheduled for August 13, 2025 at 3:00 pm ET. CMS is interested in obtaining our partners' feedback based on your experiences with other insurers regarding real-time claims processing integration and solutions in the industry (e.g. revenue cycle health, denials, rejections, appeals, reimbursement time frames).

CMS also wants to hear your feedback to improve and enhance CMS processes related to Strengthening Medicare's EDI cybersecurity controls to better protect the integrity and availability of information systems involved in processing Medicare claims as well as the security and privacy of the sensitive beneficiary data being exchanged.

In both topics of interest, CMS would like to specifically hear your thoughts and ideas regarding:

- Harnessing technology such as artificial intelligence and other tools for claims processing, automation, prior authorization, and payment
- Self-service transactions (e.g. website/portal/interactive voice response unit)
- Your experience with Medicare in relation to or compared with other payers with regard to claims processing timeframes, speed of payments, access to tools and resources in the event of disruptions to your billing operations, and related topics that are important to your revenue cycle management.
- Any operational, organizational, financial or regulatory challenges you have experienced related to real-time claims processing.

CMS wants to hear from you…REGISTER TODAY! Spots are limited.

You may email comments/questions in advance of the listening session to cmslistens@cms.hhs.gov with "**Real-Time Claims & EDI Cybersecurity**" in the subject line. We may address them during the listening session or use them to develop other resources following the session.

Background

Real-Time Claims: CMS is in the early stages of developing a pilot to process claims faster, with a long-term goal of working toward increased certainty of payment for providers in exchange for clinical data. CMS is interested in helping providers and payers to take better care of beneficiaries, their patients, members, and decreasing the resources needed to manage their revenue cycles with denials, appeals, and resubmissions of claims to Medicare.

EDI Cybersecurity: In February of 2024, a nationwide cyberattack disabled operations of a company named Change Healthcare and had significant cascading and disruptive effects on the revenue cycle of healthcare providers, certain healthcare technologies, and clinical authorizations across the healthcare

This document presents background information on an issue that will likely be presented for future decision-making.

sector. The cyberattack on Change Healthcare hampered healthcare billing and payment operations and other processes across the healthcare industry nationwide, directly impacting approximately 400,000 Medicare providers and suppliers. In response to this attack, CMS temporarily disconnected EDI systems access for Change Healthcare billing vendors to mitigate the risk of exposing the Medicare systems environment to the cyberattack and protect the integrity of the Medicare program.

After the Change Healthcare cyberattack, CMS convened an EDI Cybersecurity Workgroup to explore options for strengthening EDI enrollment requirements and messaging to hold billing agents and clearinghouses accountable for information security. The workgroup incorporated information gathered from lessons learned to better understand stakeholder cybersecurity posture and capabilities to enable CMS and the MACs to better respond to future cyberattacks.

Target Audience: Medicare FFS providers, practitioners, suppliers, their representative associations, third party billing vendors (e.g. clearinghouses/billing and coding services, etc.), and any interested partners.