

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C4-22-04
Baltimore, Maryland 21244-1850



CENTER FOR MEDICARE

DATE: December 11, 2024

TO: Current and Future Medicare Advantage Organizations, Program of All-Inclusive Care for the Elderly Organizations, 1876 Cost Plans, and Prescription Drug Plan Sponsors

FROM: Vanessa S. Duran, Director
Medicare Drug Benefit and C & D Data Group

Kathryn A. Coleman, Director
Medicare Drug & Health Plan Contract Administration Group

SUBJECT: Reminder of Obligations to Safeguard Protected Health Information and to Continue Business Operations following a Cyberattack

A recent cyberattack on Change Healthcare, a large health payment processing company, interrupted payment processing for millions of healthcare providers and patients for several weeks and had downstream impacts on numerous functions, including electronic claim submissions and retrieval of medical records for Health Care Effectiveness Data and Information Set (HEDIS) measures. Additionally, the attack compromised protected health information (PHI) for as many as one third of Americans.¹ Several smaller incidents have also impacted health plans.

CMS is issuing this memo to remind Medicare Advantage organizations (MAOs), Part D sponsors, section 1876 cost plans, and Program of All-Inclusive Care for the Elderly (PACE) organizations of their legal obligations to safeguard PHI and to maintain business operations, such as payment processing, following any natural or manmade disasters, including cyberattacks.² CMS has observed a varying degree of cyber resiliency from MAOs, Part D sponsors, and their vendors across these

¹ Senate Finance Committee hearing “Hacking America’s Health Care: Assessing the Change Healthcare Cyber Attack and What’s Next” available online at <https://www.finance.senate.gov/hearings/hacking-americas-health-care-assessing-the-change-healthcare-cyber-attack-and-whats-next>.

² According to the Computer Security Resource Center at the National Institute of Standards and Technology, a cyberattack is “any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.” Available at https://csrc.nist.gov/glossary/term/cyber_attack.

NOTE: This document contains links to non-United States Government websites. We are providing these links because they contain additional information relevant to the topic(s) discussed in this document or that otherwise may be useful to the reader. We cannot attest to the accuracy of information provided on the cited third-party websites or any other linked third-party site. We are providing these links for reference only; linking to a non-United States Government website does not constitute an endorsement by CMS, HHS, or any of their employees of the sponsors or the information and/or any products presented on the website. Also, please be aware that the privacy protections generally provided by United States Government websites do not apply to third-party sites.

cyberattack cases.³ Often, cyber resiliency has been limited by an overreliance on a single vendor for key business functions. This situation has been exacerbated by industry consolidation and vertical integration issues underscored more broadly in the President’s “Promoting Competition in the American Economy” Executive Order 14036 of July 9, 2021.⁴ In some cases, MAOs and Part D sponsors have inappropriately focused on asking for waivers of regulatory requirements rather than focusing on increasing the cyber resiliency of their operations.

Background Regarding Recent Cyberattacks

According to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), there has been a 93 percent increase in large health data breaches reported from 2018 to 2022 (369 to 712), with a 278 percent increase in large breaches reported involving ransomware.⁵ The most common reason (generally about three-quarters) reported for a breach is from hacking, where unauthorized access to electronic equipment or a network server has taken place.⁶ As of January through August 2024 alone, there have been 396 hacking cases reported that involve at least 500 persons per case, impacting almost 43.5 million persons in aggregate.⁷

On February 21, 2024, Change Healthcare’s parent company reported that a ransomware group had conducted a cyberattack that compromised the integrity of its information systems and potentially exposed the PHI of a large number of patients.⁸ Change Healthcare took many of its information systems offline to mitigate the damage, which resulted in the company being unable to conduct key functions such as processing claims and payments for healthcare providers.⁹ As a result, many healthcare providers were unable to bill for services and many patients enrolled in health plans served by Change Healthcare were unable to access pharmacy benefits.¹⁰ Change Healthcare provides claims and payment processing services for many MAOs, Part D sponsors, Cost plans, and PACE organizations, and often their contracted hospitals and pharmacies. Thus, the cyberattack also interrupted services for many Medicare beneficiaries enrolled in those plans. Systems critical to payment and claims processing were not restored until mid-March or early April and other systems took even longer to restore.¹¹ The financial problems that healthcare providers and pharmacies experienced as a result of the interruption in payments are in some cases still being resolved.¹²

³ Cyber resiliency is defined as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. National Institute of Standards and Technology, Computer Security Resource Center, glossary available at https://csrc.nist.gov/glossary/term/cyber_resiliency.

⁴ 86 FR 36987, available online at <https://www.govinfo.gov/content/pkg/FR-2021-07-14/pdf/2021-15069.pdf>

⁵ Administration of Strategic Preparedness and Response, U.S. Department of Health and Human Services, “Healthcare Sector Cybersecurity,” December 2023, available at <https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf>.

⁶ Office for Civil Rights, U.S. Department of Health and Human Services, “Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022,” available at <https://www.hhs.gov/sites/default/files/breach-report-to-congress-2022.pdf>.

⁷ Analysis of Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information reports from 1/1/2024 to 8/31/2024. Available online at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

⁸ Congressional Research Service, “The Change Healthcare Cyberattack and Response Considerations for Policymakers”, April 24, 2024, available at <https://crsreports.congress.gov/product/pdf/IN/IN12330>.

⁹ Id.

¹⁰ Id.

¹¹ See United Health Group webpage “Information on Change Healthcare Cyber Response” at <https://www.unitedhealthgroup.com/ns/changehealthcare.html>, last accessed December 3, 2024.

¹² Id. See also “Responses to Questions for the Record for Andrew Witty”, U.S. Senate Committee on Finance, Full Committee Hearing, May 1, 2024, available at https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf.

Organizations' Obligations to Protect PHI

MAOs, Part D sponsors, Cost plans, and PACE organizations are required by federal law, regulations, and their contracts with CMS to safeguard enrollee PHI.¹³ The Privacy Rule at 45 CFR Part 160 and Part 164, Subparts A and E, adopted pursuant to Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §§ 1320d -1320d-9) protects PHI, which generally includes “individually identifiable health information” held or transmitted by a covered entity or its business associate in any form, electronic or paper. 45 CFR § 160.103. The HIPAA Security Rule also requires covered entities and business associates to “ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity or business associate creates, receives, maintains, or transmits” and to “protect against any reasonably anticipated threats or hazards to the security or integrity of such information.” 45 CFR § 164.306(a)(1) & (2). Medicare regulations 42 CFR §§ 422.504(h)(2) & 423.505(h)(2) require MAOs and Part D sponsors to abide by the HIPAA Privacy Rule. Additionally, 42 CFR §§ 422.118(a) & 423.136(a) require MAOs and Part D sponsors to establish procedures to “[a]bide by all Federal and State laws regarding confidentiality and disclosure of medical records, or other health and enrollment information.” They also “must safeguard the privacy of any information that identifies a particular enrollee.” 42 CFR §§ 422.118(a) & 423.136(a). Furthermore, those organizations that are Part D sponsors must comply with the privacy requirements of 42 CFR Part 423, and PACE organizations must safeguard the privacy of patient information as required by and described in 42 CFR § 460.200. CMS may take compliance or enforcement action against any of these organizations that fail to comply with the privacy and security requirements of their contract with CMS, or (in the case of PACE organizations) their program agreement with CMS and the state administering agency.

MAOs and Part D sponsors are responsible for ensuring that their first tier, downstream, and related entities (FDR) comply with all requirements of the MA and Part D regulations and their contracts with CMS. FDRs include any parties that MAOs and Part D sponsors contract with, directly or indirectly, to perform administrative services or health care services for their enrollees.¹⁴ These include, but are not limited to, payment and claims processors such as Change Healthcare. Under 42 CFR §§ 422.504(i)(1) and 423.505(i)(1), an MAO or Part D sponsor “maintains ultimate responsibility for adhering to and otherwise fully complying with all terms and conditions of its contract with CMS”, notwithstanding any relationships that they may have with their FDRs. Each and every contract that an MAO or Part D sponsor has with an FDR must contain a provision requiring any services performed pursuant to that contract to be “consistent and comply with the [MAO’s or Part D sponsor’s] contractual obligations.” 42 CFR §§ 422.504(i)(3)(iii) & 423.505(i)(3)(iii). Additionally, each and every contract with an FDR must specify that the MAO or Part D sponsor monitors the performance of the FDR on an ongoing basis. 42 CFR §§ 422.504(i)(4)(iii) & 423.505(i)(4)(iii). Cost plans and PACE organizations that are also Part D sponsors must comply with the requirements for FDRs in 42 CFR Part 423.

MAOs and Part D sponsors thus must not only themselves comply with the Privacy Rule and other applicable requirements to safeguard PHI, but they must monitor and ensure their FDRs’ compliance. CMS can take enforcement and/or compliance action against any MAO or Part D sponsor whose FDR fails to comply with these requirements just as if the MAO or Part D sponsor itself had directly failed

¹³ Although CMS is discussing some of the important regulatory requirements in this space, this section is not intended to be a comprehensive review of existing laws protecting PHI. The HHS Office for Civil Rights (OCR) is responsible for promulgating and enforcing the HIPAA Privacy and Security Rules.

¹⁴ See the definitions of “downstream entity”, “first tier entity”, and “related entity” at 42 CFR §§ 422.2 & 423.4.

to comply. Therefore, CMS strongly encourages MAOs and Part D sponsors to monitor their FDRs' efforts to safeguard PHI, including their efforts to guard against future cyberattacks.

Organizations' Obligations to Maintain Business Operations

MAOs, Part D sponsors, and Cost plans contract with CMS, and PACE organizations enter agreements with CMS and the state administering agency, to provide health coverage to enrollees in their respective plans or programs in accordance with the requirements delineated in the Social Security Act, federal regulations, CMS guidance, and their contracts with CMS or PACE program agreements with CMS and the state administering agency. These requirements include, depending on plan type:

- Providing enrollees coverage and, if applicable, delivery of health benefits and services as required by 42 CFR Part 417 Subpart O, Part 417 Subpart U, Part 422 Subpart C, or Part 460 Subpart F.
- Providing coverage of Part D drugs and benefits as required by 42 CFR Part 423 Subpart C.
- Paying "clean claims" from medical providers, pharmacies, and others in accordance with the prompt pay requirements at 42 CFR §§ 422.520 and/or 423.520.
- Providing Part D benefits by means of a point of service system to adjudicate drug claims in a timely and efficient manner in compliance with CMS standards, in accordance with 42 CFR § 423.505(b)(17); and
- Processing enrollments and disenrollments as required by 42 CFR Part 417 Subpart K, Part 422 Subpart B, Part 423 Subpart B, and/or Part 460 Subpart I.

Contract requirements usually remain in effect even when complying with them is difficult due to circumstances outside organizations' immediate control, such as a natural or man-made disaster. CMS grants some flexibilities during a disaster or emergency – for example, the special requirements applicable for MAOs during a disaster or emergency as described at 42 CFR § 422.100(m) or the various flexibilities CMS permitted for MAOs, Part D sponsors, and others during the COVID-19 public health emergency. However, CMS does not typically grant these flexibilities outside the context of an emergency declared by the President under the Stafford Act or National Emergencies Act, a public health emergency declared by the Secretary of Health and Human Services ("Secretary") under the Public Health Service Act, or an emergency declaration by the Governor of a state. Neither the President nor the Secretary declared an emergency under those authorities as a result of the Change Healthcare cyberattack. Therefore, unless there is a formal emergency declaration from the President or Secretary, CMS would generally expect organizations to continue to comply with their contractual obligations even when their ability to do so is affected by a cybersecurity incident that compromises their normal business operations.

Notwithstanding this expectation, CMS recognizes that a variety of emergencies can temporarily prevent an organization from continuing normal operations. For this reason, CMS requires MAOs and Part D sponsors to develop, maintain, and implement business continuity plans that meet the requirements of 42 CFR §§ 422.504(o) & 423.505(p). These include planning to continuously operate or, in the event of failure, restore on a timely basis information technology systems, including those supporting claims processing at point of service (42 CFR §§ 422.504(o)(1)(ii)(B) and 423.505(p)(1)(ii)(B)).¹⁵ Cost plans and PACE organizations that are also Part D sponsors must comply with the business continuity planning requirements in the Part D regulation. CMS also requires PACE

¹⁵ CMS previously noted these requirements as they relate to cyberattacks in the March 6, 2024, HPMS memorandum "Addressing Impacts Related to the Cyberattack on Change Healthcare."

organizations to prepare for emergencies as described in 42 CFR § 460.84. CMS has observed that plans demonstrating superior cyber resiliency have reported having backup vendors and/or internal capacity for key business operations at risk for an attack. While this is not a specific requirement that MAOs and Part D sponsors must follow, CMS notes this approach as best practice.

While compliance with continuity planning requirements does not relieve organizations of their responsibility to continue operating as required by their contracts with CMS, failure to plan may delay restoration of any interrupted functions. Failure to comply with planning requirements could also result in compliance or enforcement action in addition to any actions taken as a result of an organization's failure to operate in accordance with other contract or program agreement requirements during an emergency. CMS, therefore, urges organizations to review and update their plans as necessary to prepare for future emergencies, including cyberattacks such as the Change Healthcare cyberattack.

Vendor reporting in the Health Plan Management System (HPMS)

CMS reminds MAOs and Part D sponsors to keep updated their FDR vendors in the Part C/D Information section of the Basic Contract Management module in HPMS. MAOs and Part D sponsors can expect that their CMS Account Managers will discuss their cyber resiliency plans, including the risks presented by FDR vendors and the business continuity plans should a cyberattack occur. Note that CMS may enhance these reporting requirements in the future. Any such enhancement would be subject to the normal Paperwork Reduction Act (PRA) notice and comment process.

Recommended Practices

In addition to the requirements and expectations outlined in this memo, we encourage MAOs, Part D sponsors, Cost plans, and PACE organizations to follow guidance provided by the U.S. Department of Health and Human Services' (HHS) Cyber Performance Goals¹⁶ and the President's National Security Memorandum-22.¹⁷

The HHS Cyber Performance Goals promote enhanced cyber resilience across the entire health care and public health critical infrastructure sector. HHS published these voluntary healthcare specific goals to help healthcare organizations prioritize implementation of high-impact cybersecurity practices. At minimum, MAOs, Part D sponsors, Cost plans, PACE organizations and their FDRs should strive to adhere to the "essential" goals within the next 12 months and the "enhanced" goals in the next 2 years. While CMS strongly recommends adoption of these goals, they are voluntary at this time.

The National Security Memorandum-22, published in April 2024, further supports these cybersecurity efforts. Specifically, it assists in identifying single points of failure within healthcare critical infrastructure used to support payments by plans to providers. CMS recommends that MAOs, Part D sponsors, Cost plans, and PACE organizations consult this memorandum as they develop and implement their cyber resiliency plans.

¹⁶ <https://hhscyber.hhs.gov/performance-goals.html>.

¹⁷ <https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/>