Cooperative Exchange
The National Clearinghouse Association

Jan 31, 2025

To: Senate Finance Committee Bipartisan Staff

RE: Cooperative Exchange comments on draft policies for clearinghouse cybersecurity and enrollments

The Cooperative Exchange is pleased to provide some additional comments to the Senate Finance Committee staff on the draft policies related to clearinghouse cybersecurity practices and related enrollment procedures.

The Cooperative Exchange is comprised of 21 of the leading clearinghouses in the country, and our members provided input into these comments through the activities of our Industry Affairs Committee and our CyberSecurity and Privacy Committee. All CE members had the opportunity to provide input into our comments to provide a consensus opinion in what we are able to share with you.

The information provided includes an executive summary of our comments, along with detail supporting each of the comments. The Cooperative Exchange greatly appreciates the opportunity to provide feedback to the committee, and welcomes any additional questions that you may have.

Sincerely,

Pam Grosze, Board Chair, The Cooperative Exchange,
Vice President, Product Manager Lead, PNC Healthcare

January 31, 2025

To: United States Senate Finance Committee

RE: Senate Finance Committee draft Bill to amend **title XVIII of the Social Security Act to strengthen health care clearinghouse cybersecurity and streamlining provider enrollment into clearinghouses**

Cooperative Exchange Comments Section One:

The Cooperative Exchange (CE) Cybersecurity and Privacy Committee appreciates the opportunity to provide comments on the draft Senate Finance Committee Bill to amend title XVIII of the Social Security Act to strengthen health care clearinghouse cybersecurity. The Cooperative Exchange, the National Clearinghouse Association is composed of 21 member organizations[1], representing over 90% of the clearinghouse industry that supports over 1 million provider organizations, through more than 7,000 payer connections and 1,000 Health Information Technology (HIT) vendors, and processes over 6 billion transactions annually.

The members of the Cooperative Exchange have a personal stake in strengthening the healthcare cybersecurity infrastructure as it is a vital part of our mission to promote the effective security of the electronic exchange of healthcare data. Our objective is to ensure an uninterrupted flow of the financial resources necessary to keep the critical healthcare sector operating. We will be following the progress of this Bill with great interest and would be pleased to continue to serve as an industry resource, should the Senate Finance Committee find it beneficial.

Executive Summary

The draft Bill to amend title XVIII of the Social Security Act is a commendable step towards strengthening health care cybersecurity. We agree with the Senate Finance Committee (SFC) that establishing minimum security and resiliency standards as well as regular testing and audits for all healthcare organizations (Covered Entities and Business Associates) are critical measures to protect sensitive health information and ensure continuity of care. The following is a high-level summary of the Committee 's comments and recommendations for consideration:

[1] The views expressed herein are a compilation of the views gathered from our member constituents and reflect the directional feedback of most of its collective members. CE has synthesized member feedback, and the views, opinions, and positions should not be attributed to any single member and an individual member could. disagree with all or certain views, opinions, and positions expressed by CE.

- **Scope and Applicability**: The Cooperative Exchange is concerned that the bill's scope is limited to clearinghouses and rather than addressing Covered Entities and Business Associates, all of whom are crucial in handling protected health information (PHI). Of note, under HIPAA, clearinghouses have a dual designation as Covered Entities and Business Associates.
- **Effective Date Concerns**: January 1, 2026, effective date is considered overly ambitious due to the extensive work and costs required for compliance. Should the SFC choose to move forward, we recommend aligning an effective date with the *NPRM HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information* (NPRM HIPAA Security Rule).
- **Existing Regulatory Framework**: The document highlights existing regulations, such as the Healthcare Insurance Portable Insurance Act (HIPAA),[2] Health Information Technology for Economic and Clinical Health Act (HITECH),[3] and National Institute of Standards and Technology (NIST) standards,[4] which already provide comprehensive cybersecurity guidelines. The draft Bill should reference these regulations and standards rather than creating new requirements to avoid regulatory redundancy.
- **Business Disruption and Failover**: The Cooperative Exchanges appreciates the proposal for cooperative agreements for failover during outages but notes that existing HIPAA regulations already mandate such agreements. We recommend referencing current standards.
- **Transparency in Reporting**: The bill should balance confidentiality and transparency in reporting cybersecurity incidents, referencing existing HIPAA and NIST guidelines for guidance.
- **Incident Response Plan**: The bill should align with existing HIPAA and NIST standards for incident response plans to avoid regulatory redundancy.
- **Periodic Review of Standards**: The bill should establish a mechanism for periodic review and updating of security and resiliency standards by OCR, recommending a 12-month review cycle.
- **Disaster Recovery and Business Continuity**: The focus on resiliency in disaster recovery (DR) and business continuity planning (BCP) is emphasized, noting the difference in recovery times between standard events and ransomware attacks. We recommend aligning with the existing HIPAA and NIST DR and BCP specification requirements to mitigate regulatory redundancy.
- **Third-Party Audit Oversight**: The bill should include provisions for third-party audit oversight to ensure accountability and compliance with cybersecurity standards, referencing existing HIPAA and HITECH requirements.

The following provides additional content to the recommendations referenced above, as well as a few points which we would like to bring to the Committee's attention that require further consideration.

Comment and Recommendations:

General Comment on Bill Scope Applicability:

While we appreciate the Senate Finance Committee focus on improving cybersecurity, one we also share, we are concerned about the limited scope of the Bill in addressing only clearinghouses, rather than addressing Covered Entities and Business Associates, which would include the broad healthcare ecosystem. Under HIPAA, clearinghouses are designated as a Covered Entity, and we additionally serve as Business Associates for the majority of our customers.

When acting as a Covered Entity, we may use third party vendors (Business Associates) services, which may require access to PHI to perform certain functions on behalf of a Covered Entity. The Department of

---

[2] HIPAA Insurance Portability and Accountability Act : https://www.hhs.gov/hipaa/index.html

[3] Health Information Technology for Economic and Clinical Health Act (HITECH): https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

[4] National Institute of Standards and Technology (NIST): https://www.nist.gov/

Health and Human Services (HHS) requires any Business Associate that stores, processes, transmits, maintains, and/or touches protected health information (PHI) in any way be HIPAA compliant.[5] Under HIPAA, Covered Entities and Business Associates are legally bound to protect PHI and comply with HIPAA rules (e.g., Security, Privacy, and Breach Notification).

In an interconnected healthcare system, cybersecurity does not rely on one party; rather, cybersecurity is only as good as the weakest party in the chain. Consequently, applying cybersecurity requirements to clearinghouses only, rather than more broadly to all healthcare actors will not ensure a secure healthcare system. To achieve the SFC objectives of strengthening healthcare cybersecurity, we recommend expanding the scope to include Covered Entities and Business Associates to align with the HIPAA Security and Privacy, HITECH, and Breach Notification rules, as both entities are interdependent of each other in the data exchange of Protected Health Information (PHI) and Individual Identified Health Information (IIHI).

January 1, 2026, Effective Date:
The January 1, 2026, deadline is not realistic given the amount of work that must be undertaken by healthcare entities and the costs associated therewith, particularly given other state and federal laws, such as the NPRM HIPAA Security Rule, which will require Covered Entities and Business Associates to enhance technical and operational security controls. We recommend the effective date aligns with the NPRM Security Rule effective date to mitigate regulatory redundancy.

Section 2 (l)(2)(A) Minimum Security and Resiliency Standards

Existing Regulatory Oversight:
It is crucial to acknowledge the existing regulatory framework governing healthcare cybersecurity. The Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy Rules, along with the HITECH Act, NIST Cybersecurity Framework 2.0 Standards, and NIST SP-800 53Rev5 Security and Privacy Controls for Information Systems and Organizations, have established comprehensive cybersecurity minimum security standards and resiliency standard for HIPAA regulated Covered Entities and Business Associates, which includes clearinghouses. These are the same minimal security and resilience standards as draft in the Bill.

While there are existing federal cybersecurity regulations and enforcement of the cybersecurity rules, we also recognize the need to update the 2013 HIPAA Security regulations to address the gaps in identified cybersecurity controls and regulations to meet the ever-increasing cybersecurity threats to the healthcare sector.

To address these industry cybersecurity gaps, on January 6, 2025, OCR published the NPRM HIPAA Security Rule. [6] The Rule aims to modernize cybersecurity requirements, bridge compliance gaps, and tackle evolving threats with new administrative, technical, and physical safeguards. Key features include mandatory encryption, enhanced access controls, expanded risk analysis requirements, and revised Business Associate agreement obligations. Rather than the Bill setting the floor for cybersecurity requirements, we recommend that the Bill specify a recurring schedule for OCR to make such updates, e.g. every two years, so that the industry can continue to meet evolving cybersecurity threats.

---

[5] May 24, 2019, HHS Definition of Business Associate: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html
[6] January 6, 2025 HHS NPRM HIPAA Security Rule to Strengthen Cybersecurity of Electronic Protected Health Information: https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information

Specificity and Consistency of Standards:
While the bill mandates minimum security and resiliency standards, it lacks specific details. Our recommendation would be for the Bill to explicitly reference existing HIPAA Security and Privacy rules, HITECH and NIST minimal security and resiliency standards, to ensure consistency and mitigate regulatory redundancy. These requirements should be applied to both Covered Entities and Business Associates to align with existing regulations and standards.

Section 2(B)(III)(ii) Cyber Recover Plan (I)

Cooperative Agreement:
The HIPAA and HITECH regulations require Covered Entities and Business Associates to execute a Trading Partner Agreements (cooperative agreement), which are currently in place between all clearinghouses, incorporate BAAs, and ensure that clearinghouses can securely share transactions with each other. cooperative agreement Business Associate Agreement (BAA). The purpose of the BAA is to protect the data and ensure that any party who performs functions/activities on behalf of the Covered Entity will handle PHI in adherence to HIPAA Rules and standards to protect the data.[7] The BAA also defines the contractual obligation of the Business Associate to comply with specified business continuity, disaster recovery, breach notification reporting timelines and terms of contractual termination. Trading Partner Agreements, which are currently in place between all clearinghouses, incorporate BAAs, and ensure that clearinghouses can securely share transactions with each other.

The NPRM HIPAA Security Rule, addresses additional BAA contractual controls. In addition, HHS has provided regulated entities with a Model Business Associate Agreement[8] template which includes contractual conditions for termination. We recommend in the absence of a new HIPAA Security Rule, that the Bill refers to the HHS Model Business Agreement as an industry resource.

Additional Considerations:
Business Disruption Failover Considerations: We appreciate the SFC proposal to have a cooperative agreement in place with another clearinghouse where traffic can be shifted during an outage. As noted above, cooperative agreements are already mandated under HIPAA. In the scenario, where there is a need to failover (business continuity/disaster recovery) to another clearinghouse, it is the clearinghouse customers (provider, payers or other third parties) who own the data (legal entities) as defined in a cooperative agreement, who have the authority to change transaction processing and/or other services to another clearinghouse. It is out of scope and compliance for a clearinghouse to unilaterally decide to move customer services without a cooperative contractual agreement from the customer and other third-party clearinghouse.

In addition, the draft Bill does not indicate what types of rules would have to be in place for this to work, such as pricing agreements (which could lead to monopoly behavior), technical agreements, security agreements, etc. In response to the rise of cybersecurity incidents and/or system failures, many providers and payers are securing their own secondary clearinghouse contracts, giving them the ability to move their traffic as needed. This would allow, at the direction of the customer, cooperative agreements to be updated to implement failover requirements and ensure contractual agreements are in place with all parties. We believe this is the better path forward as it enables the users to expedite

[7] May 24,2019 HHS Definition of Business Associate: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html
[8] HHS Business Associate Model Agreement: https://www.hhs.gov/sites/default/files/model-business-associate-agreement.pdf

their business continuity plan based on their financial, technical, and security business needs. In the absence of updated HIPAA regulations, we recommend the Bill references the existing HIPAA, HITECH and NIST cooperative agreement control requirements.

Transparency in Reporting:
The Bill should balance confidentiality and transparency in reporting requirements. It should provide insights into the overall state of cybersecurity in healthcare without jeopardizing sensitive data. The NPRM HIPAA Security Rule provides additional transparency reporting guidance and requirements for Covered Entities, Business Associates, and other third-party vendors. In the absence of an updated HIPAA Security Rule, we recommend the cooperative agreement references the existing HIPAA, HITECH ACT, NIST Cybersecurity Framework 2.0, HIPAA Breach Notification Timelines, and NIST SP 800-66r2 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

Timeliness Reporting:
Often providers are not direct customers of clearinghouses (this is dependent on each clearinghouse's business model). Rather, clearinghouse customers may include other contractual party entities Electronic Medical Record Vendors (EMRs) and Revenue Cycle Management Vendors (RCM) who provide the clearinghouse services as part of their platform. When clearinghouses work with a channel partner such as an EMR vendor, the clearinghouse is prohibited from directly contacting the providers that are the customer of the EMR vendor, nor does the EMR vendor provide contact information to the clearinghouse. In the event of a cybersecurity incident, clearinghouses notify their direct customers (in this case an EMR vendor with whom they are contracted) and the customer is expected to notify their users.

We are concerned with the Committee's draft requirements on notifications and maintaining contact lists, which would be unimplementable as our contracts may legally prohibit us in meeting this requirement. There is no clear regulatory guidance regarding this type of contractual scenario which can impede stakeholder notification. We recommend the Bill address third- party vendor notification requirements, as specified in the NPRM HIPAA Security Rule, which addresses this contractual gap by requiring Business Associates who receive a notification to provide such notification to their Covered Entities.

Incident Response Plan:
The HIPAA Security and Privacy rule requires Covered Entities and Business Associates to develop and maintain a comprehensive incident response plan. The NIST SP800- 53 Rev5 Security and Privacy Controls for Information Systems and Organizations (HIPAA requirement) and the NIST Cybersecurity Framework 2.0 Standards provide additional guidance regarding Incident Response Plan required controls in order to mitigate risk. We recommend the Bill aligns with the existing HIPAA regulations and NIST Standards to mitigate regulatory redundancy.

Periodic Review of Standards:
The Bill should establish a mechanism for the periodic review and updating of security and resiliency standards. We recommend the Bill aligns with the NPRM HIPAA Security Rule which recommends a 12-month maintenance review cycle.

Focus on Disaster Recovery and Business Continuity:

The draft Bill emphasizes the importance of "resiliency" in the context of disaster recovery (DR) and business continuity (BC) planning, rather than breach notification. This distinction is crucial, as breach notification requirements are already addressed under existing HHS regulations.

In addition, it is essential to acknowledge the difference between the recovery time for a standard disaster event, such as a data center outage, and a ransomware event. Standard DR Recovery processes cannot be followed during a ransomware event. In the event of a ransomware attack, the steps required to restore services increase and may include a thorough third-party forensics investigation of the environment, environment rebuilding and third-party assessments to attest that the environment is clean. These additional requirements significantly extend recovery timelines to anywhere between 12-16 weeks. In addition, there needs to be consideration regarding external regulatory investigations, such as the FBI, Homeland Security, and other enforcement entities, which may not allow any outside communication due to compromising their investigation, which places legal constraints in our ability to comply with industry reporting requirements. We recommend that the SFC work with the FBI and Homeland Security to better understand the investigative processes following a ransomware attack in order to put in place appropriate requirements and timelines.

Timeframe Alignment and Industry Standards:
The proposed 48-hour timeframe for recovery from a standard event, such as a data center outage, should be aligned with industry standards and best practices, and address exceptions for external investigation as referenced above (FBI and other law enforcement entities). The following are regulatory resource references:

- **NIST SP 800-53 / Cybersecurity 2.0 Framework:** Provides comprehensive guidance on cybersecurity risk management, including incident response timelines based on type of incident and severity level.
- **NIST SP 61 Rev 3:** Offers recommendations and considerations for incident response, including timelines for discovery, and remediation based on type and severity of incident.
- **CISA Guidelines:** Specifies a 48-hour timeframe for incident reporting, aligning with the draft Bill's timeframe.
- **NPRM HIPAA Security Rule**: addresses incident response and timeline for discovery based on NIST Cybersecurity Incident Recover and Response Guidelines.

Additional Recommendations
To address these points, the following language is recommended:
"To ensure operational resilience, entities must comply with the following":

- Adhere to industry standards and best practices for disaster recovery (DR) and business continuity (BC) planning, such as NIST SP 800-53 / Cybersecurity Framework 2.0 and NIST SP 61 Rev 3.
- Adhere to industry standards and best practices for disaster recovery (DR) and business continuity (BC) planning, such as NIST SP 800-53 / Cybersecurity Framework 2.0 and NIST SP 61 Rev 3.
- Establish and maintain incident response plans that include defined timelines for discovery, remediation, and reporting, aligning with CISA guidelines and state-specific requirements.
- For TPAs and BAAs ensure service level agreements (SLAs) are consistent with HHS breach notification timelines and remediation requirements.

Section (a)(I)(C) Annual Independent Security Audit and Stress Test Requirements

Third-Party Audit Oversight:
The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) requires HHS to periodically audit covered entities for regulatory compliance with the requirements of the HIPAA Privacy, Security, and Breach Notification Rules.

In addition, the HIPAA Security Rules and HITECH Act require Covered Entities and Business Associates, as part of the required risk assessment controls, to conduct an internal audit annually. We recommend the Bill should include provisions to align with the above stated regulator and standards. The NPRM HIPAA Security Rule does provide additional guidance on third- party oversight. The Bill should also address the lack of regulatory oversight of third-party auditors to ensure accountability and compliance with cybersecurity standards.

The following are additional Third-Party Audit oversight considerations to further strengthen industry cybersecurity controls and regulatory harmonization:

- Establish and mandate one national integrated cybersecurity standard to mitigate the gaps between the varies security and regulatory standards.
- Establish standardized control requirements utilizing standard frameworks, such as The National Institute for Standards and Technology (NIST) as the basis of security auditing to reduce the burden on vendors where auditors and/or regulatory entities interpret regulations in varying ways.
- Provide standardized requirements for evidence documentation so that vendors may create one response for each requirement to present to any auditor.
- The federal government certifies private third-party industry certification entities, so vendors have confidence when choosing an auditing service provider.

Section 2(I)(3) Application for Designation

Distinct Designation:
OCR is the distinct designation authority which oversees regulated entities (Covered Entities and Business Associates). The draft Bill requirement for a clearinghouse Distinct Designation entity is nonspecific. We recommend that the Bill references OCR as the Distinct Designation oversight entity to mitigate regulatory redundancies.

We do not believe that clearinghouses require a separate designation. Clearinghouses are already both a Covered Entity and a Business Associate regulated by OCR. Additionally, clearinghouses are required through various federal and state regulations as well as customer contracts to maintain multiple Accreditations/Certifications which require them to meet HIPAA Security rules as well as NIST requirements. We believe there is more value in the federal government certifying third-party industry certification entities, than creating a separate federal designation for clearinghouses.

Conclusion:

The Cooperative Exchange Cybersecurity and Privacy Committee appreciates the opportunity to comment on this important Senate Finance Committee Cybersecurity Bill. We strongly believe by addressing these points, the Bill can be strengthened to ensure the protection of health information and the continuity of patient care. It is crucial to leverage existing regulatory frameworks, promote transparency and accountability, and prioritize ongoing training and adaptation to respond to evolving cyber threats. In addition, we would be pleased to serve as an industry resource, should the Senate Finance Committee find it beneficial. We stand ready as an Association to continue to support

government and private sector collaborative initiatives to further strengthen cybersecurity across the healthcare sector.

Cooperative Exchange Comments Section Two:

In addition, The Cooperative Exchange (CE) Industry Affairs Committee appreciates the opportunity to provide comments on the draft Senate Finance Committee Bill to amend title XVIII of the Social Security Act to streamline provider enrollment into clearinghouses.

The members of the Cooperative Exchange work very closely with both healthcare providers and health plans to facilitate the enrollment process. Our objective is to ensure an uninterrupted flow of transactions between trading partners. We will be following the progress of this Bill with great interest and would be pleased to continue to serve as an industry resource, should the Senate Finance Committee find it beneficial.

Comments on Section 2 Streamlining Provider Enrollment into Clearinghouses:

IN GENERAL.— In order to streamline provider enrollment in a new clearinghouse to reduce the amount of time the provider is unable to send and receive claims, the Secretary shall enter into a contract with the Workgroup for Electronic Data Exchange (in this subsection referred to as 'WEDI') under which WEDI shall develop recommendations on the standards for transactions and data elements to process clinical, administrative, and financial information between providers and payers by health care clearinghouses that the Secretary should adopt under this part.

Comment: We appreciate the interest in streamlining the enrollment process for sending transactions to health plans. Enrollment changes are necessary for various reasons, including changes to provider systems and health plan systems that may require new or revised enrollments, and providers switching clearinghouses in the normal course of business. While some parts of these enrollment changes introduce challenges for clearinghouses, providers, and health plans, major barriers occur only when many providers may need to change at the same time, which may overwhelm health plan staff and resources.

Clearinghouses can assist providers and health plans in the enrollment process (and act as an agent for providers in the enrollment process when permitted to do so), but clearinghouses do not usually establish the requirements. This is a business process generally between health plans and providers. In dealing with situations that require many providers to make enrollment changes at the same time, for example a significant shutdown of any one clearinghouse, a focus should be on providing a reasonable bulk enrollment process (for example, the process defined in the latest CAQH CORE EFT and ERA Enrollment Operating Rules[9]). Any standards may be incidental to this and probably do not include clinical data. The Committee may also wish to understand that clearinghouses have already made some adjustments in their business processes to protect against potential enrollment problems.

[9] CORE Payment & Remittance EFT Enrollment Data Rule vPR.2.0 and CORE Payment & Remittance ERA Enrollment Data Rule vPR.2.0

While WEDI may be a possible convenor, we suggest the committee leave the name of the convenor off the bill, or perhaps ask HHS to select a convenor. This decision can come later.

Comments on Section 3 Streamlining Clearinghouse Enrollment Under Medicare Administrative Contractors

SEC. 3. STREAMLINING CLEARINGHOUSE ENROLLMENT UNDER MEDICARE ADMINISTRATIVE CONTRACTORS.

One challenge that clearinghouses and providers have with today's enrollment process is the fact that there are differing processes across health plans. This introduces complexities in trying to ensure compliance with each unique process to complete enrollments.

The Cooperative Exchange recommends ensuring as much consistency as possible with health plan enrollment processes. Establishing a separate, unique process for Medicare Administrative Contractors increases complexity rather than streamlining processes. We would advocate for one standard process for the industry. Therefore, section 3 should be eliminated or clarified that Medicare Administrative Contractors should follow the industry standard enrollment process. In addition, we would recommend that the turnaround time for enrollment completion should be determined through the process detailed in section 2, so addressed in that section rather than set at 5 days in section 3. The requirements for electronic signature and bulk enrollment should be addressed as part of that process in section 2 as well.

Conclusion:

The Cooperative Exchange Industry Affairs Committee appreciates the opportunity to comment on this important Senate Finance Committee Enrollments Bill. We strongly believe by addressing these points, the Bill can be strengthened to address the complexities in today's enrollment processes and streamline the process in situations where many providers must make changes at the same time. It is imperative to establish processes to facilitate management of bulk enrollments and to standardize processes across all health plan types in the industry.

The Cooperative Exchange would be pleased to serve as an industry resource, should the Senate Finance Committee find it beneficial. We stand ready as an Association to continue to support government and private sector collaborative initiatives to further strengthen cybersecurity across the healthcare sector and to address administrative processes like enrollments to facilitate exchange of transactions between all trading partners.

Thank you for the opportunity to provide feedback. Please contact us if you should have any questions regarding our comments.

Sincerely,

Pam Grosze, Board Chair, The Cooperative Exchange,

Vice President, Product Manager Lead, PNC Healthcare