601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004
T 202.778.3200
F 202.331.7487
ahip.org

Micky Tripathi, PhD MPP
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street SW, 7th Floor Washington, DC 20201

RE: AHIP Comments on the USCDI Version 3

Dear Dr. Tripathi:

Patients deserve high-quality, equitable, and affordable care, with everyone working together. This requires safe, efficient sharing of data that patients, their care teams, and their health insurance providers need to make informed health care decisions. AHIP[1] appreciates the Office of the National Coordinator for Health Information Technology's (ONC) ongoing work to advance the interoperability of health information through the United States Core Data for Interoperability (USCDI). We agree that a common set of data classes and elements is essential to achieving interoperability between consumers, doctors, hospitals, health insurance providers, and other stakeholders.

AHIP and its members strongly support moving to a health care system where data flow seamlessly among appropriate stakeholders to achieve improved wellness and better health outcomes. We support efforts to develop data standards that aim to align how information is captured by providers, payers, and other stakeholders. To that end, AHIP is committed to developing policy solutions that will support a more consumer-focused market, ensure meaningful access to actionable information, and promote quality and affordability. It is with this in mind that we offer these comments and recommendations.

Refocus the Health Insurance Information Data Class

We have significant concerns with the new Health Insurance Information data class proposed by ONC. We are unclear on the utility of the information beyond the existing, standardized, electronic, and interoperable HIPAA transaction sets. Thus, we believe the inclusion of such data elements here creates a risk to consumers without significant benefit and suggest an alternative approach.

Consumer Data Privacy and Security

As personal health information becomes more freely available, privacy and security are essential. To operationalize this commitment, AHIP's Board of Directors and its Chief Medical Officers leadership team released core guiding priorities and a detailed roadmap to further protect the privacy, confidentiality, and cybersecurity of consumer health information.[2] We use the lens of these priorities to consider the proposed policies.

[1] AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone.
[2] https://www.ahip.org/news/press-releases/ahip-outlines-priorities-and-roadmap-for-protecting-privacy-and-security-of-consumer-health-information

The information included in the USCDI must be shared by providers and most payers, at a patient's request, with third-party applications (apps) that are generally not governed by the Health Insurance Portability and Accountability Act (HIPAA) and are permitted to use data for secondary purposes. This exchange, given present technological constraints, is all-or-nothing. Thus, extreme caution should be exercised and the notion of minimum necessary applied to the inclusion of new data elements, particularly personally identifiable information such as Member Identifier, Subscriber Identifier, Relationship to Subscriber, and Group Number. Such information, when combined with current USCDI version 1 data elements, such as First Name, Last Name, Date of Birth, and Current Address, could risk a person's privacy and even safety.

As noted above, apps are not covered by HIPAA and can sell or re-use a person's data without authorization beyond the initial check box terms of service. Many consumers may not thoroughly read the terms and conditions of an app's use or fully understand the implications of sharing data outside of HIPAA. Even those who do often only have the choice of either agreeing to the terms or not using the service. As the information changes hands down a chain of entities, the privacy and security of the information become increasingly vulnerable risking inappropriate disclosure and re-identification of other data sources. Research has found that de-identified data can be accurately re-identified by correlating several data points such as a person's date of birth, zip code, and gender, potentially exposing a person's identity and medical history.[3,4] Re-identification research has found that the more data points available to support re-identification, the greater the likelihood of an accurate match. One study found that 15 demographic data points could correctly re-identify more than 99% of Americans.[5]

Given this, there should be a clear and compelling use case for each element before it is included in the USCDI. We must ask: How will this element be used to improve the health and well-being of consumers, and what are the risks associated with its disclosure? The proposed individually identifying data elements in the Health Insurance Information data class, like Member Identifier or Subscriber Identifier, are not necessary to support functions like user authentication for apps. Health care and health insurance providers have established alternative secure user identification protocols for authorized users to obtain data. Moreover, this granular level of detail poses a real threat to consumers if obtained by bad actors. ***As such, we do not support the addition of several newly proposed data elements in the Health Insurance Information data class that could expose a person's social security number, employer, and family relationships.***

<u>Disclosure of Confidentially Negotiated Rates</u>

AHIP and our members are firmly committed to providing consumers useful, appropriate price transparency to aid in their decision-making and empowering them to choose health care services that are both affordable and right for them. Most health insurance providers offer transparency tools that give consumers estimates of anticipated costs and ways to compare services based on price, quality, and

[3] https://www.theregister.com/2021/09/16/anonymising_data_feature/
[4] https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/
[5] https://www.nature.com/articles/s41467-019-10933-3?source=techstories.org

accessibility. These tools provide consumers with information that is useful to them (what can I expect to pay? Which providers are good options for me?), without risking anti-competitive consequences. In addition, the Transparency in Coverage final rule and the No Surprises Act require commercial payers to offer such cost calculators. Moreover, plans in federal programs must share claims-level data (without negotiated rates) with apps at the request of consumers as part of the Patient Access application programming interfaces (API) requirements.

We are concerned that as currently written, the proposed scope of the Coverage Status data element requires sharing of claim-level payment information through the USCDI. ***We continue to urge ONC not to force the disclosure of confidentially negotiated rates, as the inclusion of granular price information could have unintended and anti-competitive consequences.*** As noted by the Federal Trade Commission, the Department of Justice, and leading economists, requiring public disclosure of pricing data could hinder fair negotiations and drive-up consumer prices. Moreover, consumers already have access to the information they need via plan transparency tools and the Patient Access API, negating the need for this data element in the USCDI or for providers to share second-hand information through electronic health records which are not designed to accurately capture claims data. ***ONC should not include any claims-level data in the USCDI, particularly confidentially negotiated rates or any other information that could harm consumers by making public competitively sensitive information.***

<u>Alternative Approach</u>

Instead, we suggest revising the Health Insurance Information data class to focus on sharing information that can facilitate patient care, help consumers and health care providers understand coverage, assess quality, and understand the impacts of social determinants of health. A more streamlined approach could protect patient privacy, prevent the sharing of inaccurate information, and avoid market disruption. We suggest the Health Insurance Information data class focus on data elements that allow understanding of whether a person has insurance coverage, the type of coverage, and what payer(s) are covering the person. These data elements would allow health care providers to understand if a person has insurance coverage and the potential implications for care and care transitions, support quality and equity efforts, and help consumers and providers connect with health insurance provider tools for up-to-date information on the coverage of specific services. ONC should work with health insurance providers to educate consumers about the Patient Access API and other tools available to encourage data access. Leveraging these tools would ensure consumers have access to their data while protecting their identities and ensuring the information they receive is accurate and up to date.

Provide Implementation Guidance

As ONC finalizes USCDI version 3, we ask the agency to enable a clear and appropriate path toward gradual implementation of the new versions. Implementation guides must be updated by the standards development organizations (SDO) before adherence to the standards is required. Additionally, under the proposed new elements of the Patient Demographic data class, not all systems are currently set up to collect tribal affiliation, and occupation is often only available if submitted by employers. Due to the variation in the collection of this data at this time, it is important that such data reporting is not required until stakeholders have developed, tested, and implemented standards to ensure complete and

accurate collection. ***ONC and CMS should work together with SDOs to ensure a reasonable implementation timeframe based on the completion of mature standards and implementation guides*.**

Facilitate Alignment All-Payer Claims Databases with the USCDI

We encourage ONC to continue to advance data standardization in other forums to promote interoperability and data sharing across the health care industry. We appreciate ONC's work to develop and advance the USCDI and its partnerships with SDOs to facilitate its implementation. ONC should work with the Department of Labor to ensure that requirements for all-payer claims databases similarly advance interoperability and encourage alignment across data sets. For example, the prior State All-Payer Claims Databases Advisory Committee (SAPCDAC) report recommended the Common Data Layout (CDL) without encouraging alignment with FHIR standards or working with the SDOs such as HL7. ***We encourage ONC to work with DOL to encourage alignment between the CDL and USCDI to promote interoperability. To facilitate such work, HHS should encourage the DOL to work with an American National Standards Institute (ANSI) accredited SDO to maintain and update the APCD standardized reporting format.***

AHIP and its members look forward to working with ONC to continue to advance interoperability to empower patients and support patient care. If you have any questions, please contact me at (202) 778-3246 or at dlloyd@ahip.org.

Sincerely,

Danielle A. Lloyd, MPH
Senior Vice President, Private Market Innovations & Quality Initiatives

Appendix A: AHIP Comments on USCDI Vesion 3 Data Elements

Health Insurance Information	
Coverage Status	AHIP does not support the addition of the Coverage Status data element. Heretofore, the USCDI has focused on clinically relevant information in the patient medical record. As this element is specified at the claim level, it would inherently be drawn from the billing systems that already have established content and technical standards governed elsewhere. Given that payers are the source of truth for coverage information for the insured and separate rulemaking and standards address such disclosures for plans in federal programs, those subject to the USCDI standard, it should not be duplicated in the USCDI. AHIP and our members are firmly committed to providing consumers coverage and price transparency to aid in their decision-making and empowering them to choose health care services that are both affordable and right for them. However, we urge ONC to consider the potential unintended consequences of the release of claims-level data. We are concerned that the applicable proposed standards would force the disclosure of non-public, confidentially-negotiated prices. Requiring public disclosure of pricing data could have potentially negative competitive effects that could hinder fair negotiations and drive up consumer prices. According to the Federal Trade Commission (FTC), "…transparency is not universally good. When it goes too far, it can actually harm competition and consumers. Some types of information are not particularly useful to consumers, but are of great interest to competitors."[6] At the same time, this information would not provide meaningful information to consumers. Health insurance provider tools are the best source for estimates of anticipated costs and ways to compare services based on price, quality, and accessibility. Consumers are best served receiving information from health insurance providers, not second-hand through health care providers. We agree that claims-based clinical encounter data should be shared either directly or through third-party apps to support consumer longitudinal health records. By leveraging health insurance provider tools, consumers can have access to accurate and up-to-date information on the coverage status of their claims. This information would convey relevant information such as the provider name, date of service, and service list. However, this should not include provider charges or payer negotiated rates. If cost information is included, it should be limited to the cost-sharing obligation of the consumer. Only payers can accurately estimate the cost of a service and the out-of-pocket spending of enrollees based on their plan benefits. Moreover, the information obtained by apps can be sold for other purposes as long as disclosed in the terms and agreements raising the concern that large databases could be built from this competitively-sensitive information, leading to higher prices for consumers. **ONC should not include claims**

[6] Koslov, T. and Jex, E.; *Price transparency or TMI?;* Federal Trade Commission Blog; Jul 2, 2015 2:31PM; **https://www.ftc.gov/news-events/blogs/competition-matters/2015/07/price-transparency-or-tmi.**

	level information and should not require the disclosure of competitively sensitive information such as negotiated provider rates. Instead of defining this data element as "the presence or absence of coverage for a particular encounter or claim" we urge ONC to revise this element to instead focus on person's insurance status broadly. This would allow providers to understand a person's potential social risks related to a lack of health insurance and the impact that could have on their care. With this information, consumers and health care providers could work with their health insurance providers to engage in shared decision making based on accurate and current information on a person's insurance coverage.
Coverage Type	AHIP appreciates the opportunity to comment on the Coverage Type data element and we do not oppose the addition of this data element. However, ONC should ensure this data element is feasible on a national scale before included it in USCDI version 3. We note that the codeset available at http://hl7.org/fhir/R4/valueset-coverage-type.html seems to be a mix of policy types (POS/HMO/PPO) and specific benefit types (MENTPOL/DISEASE/DRUGPOL) adding complexity to choosing the correct values. These codes could be subject to interpretation and limited interrater reliability. The potential for variability in coding means this data should be used with caution. For example, comparisons of the quality of a health care or health insurance provider should only be done as specified through valid, reliable performance measures. We also encourage ONC to work with CMS, health insurance providers, and health care providers to encourage consumers to use payer tools as the source of truth for information about coverage and benefits as assumptions based on coverage type may not take into account the specific details of an individual's policy.
Relationship to subscriber	AHIP and its members wholeheartedly support moving to a health care system where data flow seamlessly among stakeholders to achieve improved wellness and better health outcomes, while at the same time ensuring privacy and security. However, as the health industry and information technology has evolved, there are both new opportunities and new threats to patient privacy. For example, sensitive patient data, at an individually identifiable level, sent from a payer to a third-party application (app) developer under these required policies can be freely sold as long as it is noted in the consumer terms and agreement. Moreover, research[7,8,9,10,11] shows that third-party health apps pose unprecedented risk to consumers' privacy given their ability to collect user data that is highly valuable to commercial interests as well as their ability to re-identify consumers in other de-identified datasets. As information included in the USCDI can be required to be shared with third-party applications that are not governed by the Health Insurance Portability and Accountability Act (HIPAA) and secondary uses of data are permitted, personally-

[7] https://www.sciencedaily.com/releases/2019/03/190321092207.htm
[8] https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636;
[9] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791
[10] https://www.washingtonpost.com/business/2019/04/22/smoking-depression-apps-are-selling-your-data-google-facebook-study-finds/
[11] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791

	identifying information should be included caution and only when necessary to support patient care. Unfortunately, third-party apps are collecting, using, disclosing, disseminating, and monetizing health data. Because technology is advancing and consumer demands are changing, the laws and regulations governing these entities vary by state, but robust privacy and security protections are generally minimal or non-existent. AHIP is concerned about the potential for bad actors to exploit data gained through the USCDI and the potential consequences for patients and their families. Consumers are often unaware of how their health data will be used or disclosed by the app developer, and frequently "click through" privacy and security fields often unwittingly granting data uses and disclosures beyond the consumer's intended purpose and often limited expectation for the purpose of the app. Many do not fully appreciate that the same robust rules that apply to some of their health care data do not necessarily apply to third-party apps. Moreover, consumers are also often unaware that the more individually identifiable data released, the easier it becomes for the de-identified database to be re-identified. Information on a person's relationship with the subscriber is not necessary for a health care provider to determine the best treatment plan for that person. However, this data element could risk providing identifying information about a person's familial relationships and its improper use could jeopardize their privacy. As such, this data element should not be included in the USCDI and instead, consumers and health care providers should work with health insurance providers to obtain information to verify a member's identity if needed.
Member Identifier	AHIP and its members wholeheartedly support moving to a health care system where data flow seamlessly among stakeholders to achieve improved wellness and better health outcomes, while at the same time ensuring privacy and security. However, as the health industry and information technology have evolved, there are both new opportunities and new threats to patient privacy. For example, sensitive patient data, at an individually identifiable level, sent from a payer to a third-party application (app) developer under these required policies can be freely sold as long as it is noted in the consumer terms and agreement. Moreover, research[12,13,14,15,16] shows that third-party health apps pose an unprecedented risk to consumers' privacy given their ability to collect user data that is highly valuable to commercial interests as well as their ability to re-identify consumers in other de-identified datasets. As information included in the USCDI can be required to be shared with third-party applications that are not governed by the Health Insurance Portability and Accountability Act (HIPAA) and secondary uses of data are permitted, personally-identifying information should be included caution and only when necessary to support patient care. Unfortunately,

[12] https://www.sciencedaily.com/releases/2019/03/190321092207.htm
[13] https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636;
[14] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791
[15] https://www.washingtonpost.com/business/2019/04/22/smoking-depression-apps-are-selling-your-data-google-facebook-study-finds/
[16] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791

	third-party apps are collecting, using, disclosing, disseminating and monetizing health data. Because technology is advancing and consumer demands are changing, the laws and regulations governing these entities vary by state, but robust privacy and security protections are generally minimal or non-existent. AHIP is concerned about the potential for bad actors to exploit data gained through the USCDI and the potential consequences for patients and their families. Consumers are often unaware of how their health data will be used or disclosed by the app developer, and frequently "click through" privacy and security fields often unwittingly granting data uses and disclosures beyond the consumer's intended purpose and often limited expectation for the purpose of the app. Many do not fully appreciate that the same robust rules that apply to some of their health care data do not necessarily apply to third-party apps. Moreover, consumers are also often unaware that the more individually identifiable data released, the easier it becomes for the de-identified database to be re-identified. A person's member identifier is a potentially personally-identifying data element and is not necessary to share to support patient care. Moreover, some consumers may have a member identifier based on their social security number. An inadvertent release of a person's social security number, combined with other data elements such as first and last name, date of birth, and current and former addresses risks their privacy and could leave a person open to identity theft. As such, this data element should not be included in the USCDI and instead, consumers and health care providers should work with health insurance providers to obtain information to verify a member's identity as needed.
Subscriber Identifier	AHIP and its members wholeheartedly support moving to a health care system where data flow seamlessly among stakeholders to achieve improved wellness and better health outcomes, while at the same time ensuring privacy and security. However, as the health industry and information technology have evolved, there are both new opportunities and new threats to patient privacy. For example, sensitive patient data, at an individually identifiable level, sent from a payer to a third-party application (app) developer under these required policies can be freely sold as long as it is noted in the consumer terms and agreement. Moreover, research[17,18,19,20,21] shows that third-party health apps pose an unprecedented risk to consumers' privacy given their ability to collect user data that is highly valuable to commercial interests as well as their ability to re-identify consumers in other de-identified datasets. As information included in the USCDI can be required to be shared with third-party applications that are not governed by the Health Insurance Portability and Accountability Act (HIPAA) and secondary uses of data are permitted, personally-identifying information should be included caution and only when necessary to support patient care. Unfortunately,

[17] https://www.sciencedaily.com/releases/2019/03/190321092207.htm
[18] https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636;
[19] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791
[20] https://www.washingtonpost.com/business/2019/04/22/smoking-depression-apps-are-selling-your-data-google-facebook-study-finds/
[21] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791

	third-party apps are collecting, using, disclosing, disseminating and monetizing health data. Because technology is advancing and consumer demands are changing, the laws and regulations governing these entities vary by state, but robust privacy and security protections are generally minimal or non-existent. AHIP is concerned about the potential for bad actors to exploit data gained through the USCDI and the potential consequences for patients and their families. Consumers are often unaware of how their health data will be used or disclosed by the app developer, and frequently "click through" privacy and security fields often unwittingly granting data uses and disclosures beyond the consumer's intended purpose and often limited expectation for the purpose of the app. Many do not fully appreciate that the same robust rules that apply to some of their health care data does not necessarily apply to third-party apps. Moreover, consumers are also often unaware that the more individually identifiable data released, the easier it becomes for de-identified database to be re-identified. A person's subscriber identifier is a potentially personally identifying data element and is not necessary to share to support patient care. As such, this data element should not be included in the USCDI and instead, consumers and health care providers should work with health insurance providers to obtain information to verify a member's identity as needed.
Group Number	AHIP and its members wholeheartedly support moving to a health care system where data flow seamlessly among stakeholders to achieve improved wellness and better health outcomes, while at the same time ensuring privacy and security. However, as the health industry and information technology have evolved, there are both new opportunities and new threats to patient privacy. For example, sensitive patient data, at an individually identifiable level, sent from a payer to a third-party application (app) developer under these required policies can be freely sold as long as it is noted in the consumer terms and agreement. Moreover, research[22,23,24,25,26] shows that third-party health apps pose an unprecedented risk to consumers' privacy given their ability to collect user data that is highly valuable to commercial interests as well as their ability to re-identify consumers in other de-identified datasets. As information included in the USCDI can be required to be shared with third-party applications that are not governed by the Health Insurance Portability and Accountability Act (HIPAA) and secondary uses of data are permitted, personally-identifying information should be included caution and only when necessary to support patient care. Unfortunately, third-party apps are collecting, using, disclosing, disseminating and monetizing health data. Because technology is advancing and consumer demands are changing, the laws and regulations governing these entities vary by state, but

[22] https://www.sciencedaily.com/releases/2019/03/190321092207.htm
[23] https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636;
[24] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791
[25] https://www.washingtonpost.com/business/2019/04/22/smoking-depression-apps-are-selling-your-data-google-facebook-study-finds/
[26] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791

	robust privacy and security protections are generally minimal or non-existent. AHIP is concerned about the potential for bad actors to exploit data gained through the USCDI and the potential consequences for patients and their families. Consumers are often unaware of how their health data will be used or disclosed by the app developer, and frequently "click through" privacy and security fields often unwittingly granting data uses and disclosures beyond the consumer's intended purpose and often limited expectation for the purpose of the app. Many do not fully appreciate that the same robust rules that apply to some of their health care data does not necessarily apply to third-party apps. Moreover, consumers are also often unaware that the more individually identifiable data released, the easier it becomes for the de-identified database to be re-identified. The information generated by the Group Number data element is not helpful outside who of payers and providers, who already have this information, and yet its disclosure could pose a risk to consumers. A person's group number is associated with a specific health insurance plan provided through an employer. When combined with another data elements in the USCDI, this data could be used to re-identify a person by detailing where that person or the person through whom he or she has coverage is employed. As such, this data element should not be included in the USCDI and instead, consumers and health care providers should work with health insurance providers to obtain information to verify a member's identity as needed.
Payer Identifier	AHIP does not support the addition of the Payer Identifier data element. While we recognize the desire to understand which payer is covering a patient, we are concerned that this data is not feasible to add to the USCDI at this time. The submission notes that there is currently no standard Healthcare Payer Identifier (e.g., HPID). While the NAIC identifier is sometimes used this is not a nationally recognized standard. A lack of standardized payer identifiers will make this data element difficult to operationalize and could introduce errors and confusion. As such, this data element should not be added to the USCDI until there is a defined, tested and accepted data standard for the payer identifier.
Health Status	
Mental Function	While we appreciate the value of information on mental function, we are concerned that as currently defined this data element may contain sensitive data that is subject to data-sharing and use restrictions under certain state laws. As such, ONC should not adopt this data element in the USCDI until potential conflicts with state or federal laws where consent or authorization is required can be resolved.
Patient Demographics	
Current Address	We appreciate the opportunity to provide feedback on the Project US@ specification as the applicable vocabulary standard for the Current Address data element. We support the use of this specification for the Patient Demographics

	data class but ask ONC and relevant stakeholders to continue collaborating to expand the address considerations to include considerations for capturing addresses for those unhoused or at transitional addresses.
Previous Address	We also appreciate the opportunity to provide feedback on the Project US@ specification as the applicable vocabulary standard for the Previous Address data element. We support the use of this specification for the Patient Demographics data class but ask ONC and relevant stakeholders to continue collaborating to expand the address considerations to include considerations for capturing addresses for those unhoused or at transitional addresses.

Appendix B: AHIP Comments on Level 2 Data Elements and Future Data Elements

Health Insurance Information	
Policy Number	As noted in our comments on the draft USCDI version 3, AHIP and our members wholeheartedly support moving to a health care system where data flow seamlessly among stakeholders to achieve improved wellness and better health outcomes, while at the same time ensuring privacy and security. However, we do not support the addition of a Policy Number data element that would be a unique identifier for a consumer's specific insurance policy. Health care providers and payer already have methods for sharing data necessary to support payment and coverage determinations. However, the disclosure of a member's specific policy number could pose a significant risk of fraud, abuse, or identity theft. As such, this data element should not be included in the USCDI and instead, consumers and health care providers should work with health insurance providers to obtain information to verify a member's coverage and benefits as needed.
Plan Identifier	We have several concerns about the feasibility of the Plan Identifier data element. First, this data element would be dependent on the Payer Identifier, which current lacks a national standard. As noted in our comments on the Payer Identifier data element, a lack of a national standard makes the Payer Identifier data element difficult to implement. Providing information on a plan type will not add value without understanding the payer supporting the plan. As such, this data element should not be added to the USCDI until national standards for payer identifiers and plan identifiers are developed and implemented.
Group Name	As noted in our comments on the draft USCDI version 3, AHIP and our members wholeheartedly support moving to a health care system where data flow seamlessly among stakeholders to achieve improved wellness and better health outcomes, while at the same time ensuring privacy and security. However, we do not support the addition of a Group Name data element that would be the name of the employer account. The information generated by the Group Name is not helpful outside who of payers and providers, who already have this information, and yet its disclosure could pose a risk to consumers. A person's Group Name is associated with a specific employer. When combined with another data elements in the USCDI, this data could be used to re-identify a person by detailing where that person or the person through whom he or she has coverage is employed. As such, this data element should not be included in the USCDI and instead, consumers and health care providers should work with health insurance providers to obtain information to verify a member's identity as needed.
Social Determinants of Health	

Outcomes	AHIP supports adding data elements to USCDI v3 that are already defined and supported by the Gravity project. ONC's site notes that the Gravity Project is currently developing corresponding value sets as well as an implementation guide for the data element and related standards. We note, however, that some of the domains listed are now outdated and not in alignment with the Gravity Project updates. For example, interpersonal Impersonal violence is now split into the categories of partner violence and elder abuse. ONC should clarify the definitions of this data element to ensure alignment with the latest updates by the Gravity Project before implementing this data element in the USCDI.
Future Data Classes or Elements	
Data Recovery/Emergency Response Preparedness	A future Disaster Recovery or Emergency Response Preparedness class could help standardize and gather data necessary to quantify impact of emergencies and assist with efficient planning and deployment of resources. We encourage ONC to facilitate a multi-stakeholder approach to further develop data elements, standards, and implementation guides**.**