AQIPS ALLIANCE FOR QUALITY IMPROVEMENT AND PATIENT SAFETY

Patient Safety Organizations and Healthcare Providers Advancing Patient Safety

March 17, 2026

Thomas Keane, MD, MBA
Assistant Secretary for Technology Policy
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street, SW
Washington, DC 20201

Re: Draft USCDI+ and USCDI v7, Data Class and Data Elements: Adverse Events, Adverse Event Outcomes, Adverse Event Recorded Time, Adverse Event Category, Adverse Event Suspected Entity and Adverse Event Degree of Harm are Categorically Excluded from Electronic Health Information (EHI) and therefore FHIR interoperability.

Dear Dr. Keane:

The Alliance for Quality Improvement and Patient Safety (AQIPS) appreciates the opportunity to comment on the Draft USCDI+ Quality Version 1 (January 2026) data elements: "adverse event," "adverse event recorded time," "adverse event category," "adverse event suspect entity" and "adverse event degree of harm" and the draft USCDI v7 "Adverse Events" data class, which includes "adverse event" and "adverse event outcomes." AQIPS is the not for profit professional association for over seventy (70) federally Listed Patient Safety Organizations (PSOs) created pursuant to the Patient Safety and Quality Improvement Act of 2005 (42 U.S.C. 299b-21 et seq., the Patient Safety Act) and their healthcare provider members. As you know, research is showing that patient safety activities are improving the quality of patient care delivery and reducing patient harm. PSOs and healthcare providers develop "provider-driven voluntary opportunities for improving patient safety for breakthroughs in our understanding of how best to improve safety." Patient Safety and Quality Improvement, Proposed Rule, 73 Fed. Reg. 8114. Toward this end, the PSO community along with their healthcare providers have developed innovative programs - including national safe-tables, peer-audit programs, best practice development collaboratives - and strategies to connect the healthcare continuum to revolutionize patient safety practice and to allow healthcare providers to confidentiality talk to each other to improve the quality of patient care.

As more fully discussed below, the New Data Class: Adverse Events (Adverse Event; Adverse Event Outcome) and the adverse event data elements cannot be accessed from the medical record, are categorically excluded from the definition of electronic

health information (EHI), and therefore are excluded from interoperability, the exchange of electronic health information.

1. **The New Data Class: Adverse Events (Adverse Event; Adverse Event Outcome) and the Adverse Event Data elements as defined by ASTR cannot be identified in the medical record because hospitals must analyze the adverse event using "patient safety activities" to determine whether an adverse event is associated with medical care. As a matter of law, "patient safety activity records" are categorically excluded from being a designated record set as defined in 45 CFR 164.501 and therefore are categorically excluded from the definition of Electronic Health Information (EHI). Additionally, Patient safety activity records are privileged and confidential under Federal privacy law (42 USC 299b-21 et seq.). As a result, failure to share adverse events and adverse event outcomes is not information blocking. Additionally, ASTR's proposal to define adverse event, adverse event outcome, adverse event recorded time, adverse event category, adverse event suspect entity and adverse event degree of harm as EHI, violates HIPAA, the Patient Safety Act and the Administrative Procedures Act (contrary to law).**

As defined by ASTR, an "adverse event" that is "harm to a patient resulting from medical care rather than the underlying disease that requires additional monitoring, treatment or hospitalization" cannot be identified in the electronic health record (EHR) because hospitals must assess whether a complication is caused by or associated with medical care or the underlying disease. This causal analysis (e.g, root cause analysis or RCA) is conducted outside of the medical record and is a Patient Safety Activity (42 U.S.C. 299b-21(5)) or other risk management or peer review process. The 21st Century Cures Act mandates standards for easier, secure sharing of electronic health information (EHI). In this regard, under 21st Century Cures Act regulations, EHI is defined as electronic protected health information (EPHI) to the extent that it would be included in a designated record set (DRS) (42 C.F.R. 170.102). Patient safety activities are categorically excluded from a DRS (45 CFR 164.501), and therefore, patient safety activity records are outside of the definition of EHI and are not subject to interoperability under the 21st Century Cures Act. The HHS final rule on information blocking, states concerning the scope of electronic health information:

> "We have adopted a focused definition of EHI in § 170.102. For context purposes, the EHI definition is focused on "electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501" with additional caveats not repeated here

> for briefness. Put simply, the EHI definition represents the same ePHI that a patient would have the right to request a copy of pursuant to the HIPAA Privacy Rule. This is a regulatory concept with which the industry has nearly 20 years of familiarity. Health IT developers' customer base includes health care providers who are HIPAA covered entities, and in many cases developers serve as HIPAA business associates to their covered-entity customers. Thus, health IT developers should be accustomed to identifying ePHI so that their products support appropriately securing it, the fulfillment of patient access requests, and the identification and reporting on breaches. They should, therefore, be well prepared to identify what EHI their product(s) would need to export in order to support a patient's HIPAA right of access."

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services (HHS), Final rule. 85 FR 25642, 25691 (May 1, 2020).

> According to the Office of Civil Rights, which is charged with enforcing HIPAA, "An individual does not have a right to access PHI that is not part of a designated record set because the information is not used to make decisions about individuals. This may include certain **patient safety activity records**, or business planning, development, and management records that are used for business decisions more generally rather than to make decisions about individuals. For example, a hospital's peer review files or practitioner or provider performance evaluations, or a health plan's quality control records that are used to improve customer service or formulary development records, may be generated from and include an individual's PHI but might not be in the covered entity's designated record set and subject to access by the individual."

HHS Guidance, Health Information Privacy: Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html (accessed May 23, 2023)(emphasis added).

Patient safety activity records (under the Patient Safety Act, 42 U.S.C. 299-21(5)) are not part of the medical record (42 USC 299b-21(7)(a)), are excluded from HIPAA's right to access regulations, are excluded from the definition of EHI and are privileged and confidential under the Patient Safety Act. The Patient Safety Act is a federal privacy statute designed in part to extend confidential peer review protections to all healthcare settings and healthcare professionals and collaborations to improve the quality of patient care through the confidential sharing of experiences and best practices among facilities using disclosure permissions (73 Fed. Reg. 8113 (Feb 2008)). All fifty (50) states have peer review statutes to implement the strong public policy that protections are necessary

for providers to implement quality/risk management system to enable healthcare organizations to identify patterns, implement preventive measures, and improve treatment protocols for the benefit of patients. The Patient Safety Act's strong, preemptive federal privilege and confidentiality (privacy) protections are intended to create a culture of safety by providing nationwide protection for comprehensive adverse event tracking across care settings, to permit self-critical patient safety analysis of quality and clinical information, and to allow for the learning and sharing of quality information to improve outcomes throughout the healthcare system. Moreover, under the Patient Safety Act, Patient Safety Activity records cannot be part of the patient's medical record (42 USC 299b-21(7)(b)).

2. **Congress designed the Patient Safety Act to allow healthcare providers to share adverse events and quality improvement best practices and protocols (e.g., a form of interoperability) to other providers to improve patient safety and the quality of patient care delivery under 42 CFR 299b-22(c)(2)(a) – Disclosures for Patient Safety Activities. Healthcare Providers that use Patient Safety Act processes meet the goals that USDCI cannot, including to support comprehensive adverse event tracking across care settings, the exchange of adverse event information so that all members of a care team are aware of previous adverse events and analyzing and reducing preventable harm in healthcare delivery.**

The Patient Safety Act is a federal privacy statute designed in part to extend peer review protections to all healthcare settings, healthcare professionals and healthcare collaborations to improve the quality of patient care and permit the sharing of experiences and best practices among facilities (73 Fed. Reg. 8113 (Feb 2008)). Congress created the Patient Safety Act to allow a form of interoperability for adverse events as well as patient safety and quality related information and best practices to be confidentially shared among healthcare providers using the Patient Safety Act's disclosure permissions to be used to improve patient safety and the quality of healthcare delivery. Many healthcare providers use AI and other technologies to identify and track events as well as analysis to use technology to prevent the event from ever occurring again in the future. Healthcare providers confidentially share patient safety activity records using the disclosure permission for patient safety activities for the benefit of patients. Additionally, healthcare providers can and do report patient complaints of harm for tracking and trending of patient provided information as well as making improvement to patient safety and patient experience. Importantly, CMS found PSOs so successful in improving patient safety and the quality of healthcare delivery that it requires hospitals to participate in PSO Patient Safety Activities as a proven best practice to improve patient safety in the Patient Safety Structural Measure. The Patient Safety Act permits the disclosure of nonidentifiable information, which is not EHI and not subject to interoperability and FHIR.

3. **The term "Adverse event" is defined in FDA regulations. FDA requires an analysis to determine whether there is an association between the event and an FDA regulated product. Again, adverse event related to FDA regulated products cannot be identified in a medical record and the resulting evaluation is a "Patient Safety Activity Record" which is categorically exempt from EHI and is confidential but may be reported to the FDA through a Congressionally established disclosure permission.**

The term "Adverse event" is defined in FDA regulations and means that the unintended harm is associated with or caused an FDA regulated medical product (21 CFR 251.2; 21 CFR 803). ASTR's materials state that "**Adverse Event** details a change to patient condition that could be an unintended effect of clinical interventions (such as medication reaction or vaccination reaction), providing essential information for patient safety monitoring and quality improvement activities. **Adverse Event Outcome** documents the patient's clinical outcome resulting from an adverse event, with examples including hospitalized, recovered, recovered with sequelae, death." FDA also has defined "serious adverse event" in 21 CFR 251.2(1). Mandatory adverse event reports by device user facilities, including hospitals, are limited to medical device deaths (see 21 CFR 803(n)); a medical device reportable event is an event that user facilities become aware of that reasonably suggests that a device has or may have caused or contributed to a death. Device and drug user facilities must report serious injury to the device/drug manufacturer or to the FDA if the manufacturer is unknown.

In its medical device reporting guidance, FDA recognizes that adverse events must be investigated to determine whether the injury was associated with the medical device. According to FDA guidance, the event must be reviewed by the user facility, including a hospital. FDA guidance states that a "Medical Device Reportable Event would not, and should not, be classified as a death unless the reporter believes the patient's cause of death was or may have been attributed to the device or the device was or may have been a factor in the death." (See FDA Guidance, Medical Device Reporting for User Facilities.) This review is a risk management or patient safety activity that is outside of the medical record and is exempt from the definition of EHI). Medication errors also need evaluation before a determination can be made whether the harm is associated with a pharmaceutical. (See 21 CFR 251.2). Therefore, adverse events are not EHI, not interoperable. Reporting mechanisms other than FHIR must be used for the mandatory reporting of medical device adverse events.

4. **Congress created a disclosure permission for providers and PSOs to disclose PSWP patient safety events that are required to be reported to the FDA under 21 CFR 801(n) so that all user facilities can comply with FDA reporting regulations and, more events can be reported after RCA evaluations. Healthcare Providers and Patient Safety Organizations also report nonidentifiable reports to FDA about medical device failures as provided under the Patient Safety Act.**

PSOs have provided a substantial number of reports to FDA concerning Medical device reportable events and other adverse events related to FDA regulated pharmaceuticals and medical devices that would not otherwise be discovered and reported. Under the Patient Safety Act, if during an investigation and root cause analysis (RCA) it is discovered that a medical device may have been the cause or contributing factor to the patient harm, the Patient Safety Act permits the user facility to report the discovered adverse event to FDA. More specifically, any information about the safety of an FDA regulated product that is required to be reported to FDA that is PSWP can be disclosed to the FDA using the FDA disclosure permission under the Patient Safety Act (42 CFR 3.206(b)(7)(i)) and the information remains privileged and confidential. To illustrate by example, a nurse told a story that a patient died and the causal factor was initially cited as failure to monitor. The duty nurse was fired. Upon conducting the Root Cause Analysis (RCA), the hospital learned that a medical device failed and this needed to be reported to the FDA (the nurse was rehired and graciously compensated). As the RCA, which is a patient safety activity record, was conducted within the hospitals Patient Safety Evaluation System, the findings with respect to the medical device/drug can be reported to the FDA through the Patient Safety Act disclosure permission (42 CFR 3.206(b)(7)(i)). Only upon conducting the RCA did the hospital learn that a medical device failed leading to the patient's death and this needed to be reported to the FDA - this PSWP could be reported to the FDA but not through the medical record because patient safety activity records the patient safety work product that it contains cannot be placed in the medical record (42 USC 299b-21(7)(a) and B), is not EHI, is not interoperable information and the hospital cannot be subject regulatory penalties for information blocking.

* * * * *

Should you have any questions or require additional information, please contact me at pbinzer@allianceforqualityimprovement.org.

Sincerely yours,

Peggy Binzer,
Executive Director and General Counsel