HANYS®
Always There for Healthcare

Marie B. Grause, RN, JD • President

Headquarters
One Empire Drive, Rensselaer, NY 12144
518.431.7600

Washington, DC Office
499 South Capitol Street SW, Suite 410
Washington, D.C. 20003
202.488.1272

June 3, 2019

Seema Verma
Administrator
Centers for Medicare and Medicaid Services
Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Don Rucker, MD
National Coordinator for Health Information Technology
Department of Health and Human Services
330 C Street, SW
Washington, DC 20201

RE: CMS–9115–P; Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers; Proposed Rule; and RIN 0955–AA01; 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program; Proposed Rule; *Federal Register* (Vol. 84, No. 42), March 4, 2019

Dear Ms. Verma and Dr. Rucker:

The Healthcare Association of New York State, on behalf of our member nonprofit and public hospitals, nursing homes, home health agencies and other healthcare providers, welcomes the opportunity to comment on the Centers for Medicare and Medicaid Services' and Office of the National Coordinator for Health Information Technology's proposed rules listed above. Due to the overlapping nature of these proposals, we are submitting our comments in a combined letter.

We appreciate the care and thought that went into this proposal. HANYS is in complete agreement with ONC's and CMS' goals of improved interoperability and patient access to health information.

On behalf of our members, we strongly support an interconnected healthcare system whereby clinicians have timely access to medical records and necessary patient information at the point of care. We recognize the imperative for patients to have easy and timely access to their medical information and data in a manner that is easily understood to best care for

themselves and their family members. HANYS strongly supports the overall intent of the CMS and ONC rules and the promise these portend for advancing the healthcare field forward in this regard.

The proposed rules represent a sea change in the framework under which healthcare providers, health insurance plans and health information technology developers and vendors capture and exchange highly sensitive health information. It is imperative that policymakers and stakeholders exercise caution to avoid unintended consequences that could arise if implementation of such policies is not thoughtful and appropriately timed. Further, an overly complex regulatory framework, if not carefully constructed, may stifle innovation and further complicate the current public-private initiatives that are taking root and accelerating change.

HANYS encourages realistic timeframes for implementation given the technical nature of the proposed changes. It is vital that there be adequate time for developing the necessary tools and ensuring providers have the operations and systems in place to use the data received from other providers.

We are commenting on certain aspects of the proposals here and offer our support for the more detailed comments of our national partner, the American Hospital Association.

HANYS' KEY RECOMMENDATIONS:

- **Interim final rules:** Given the magnitude of changes encompassed in these rules, CMS and ONC should publish interim final rules rather than final rules to allow additional opportunity for stakeholder comments.
- **Timelines:** CMS and ONC should reconsider their proposed implementation timelines, allowing appropriate time to advance the exchange of health information without creating unintended consequences or additional burden.
- **Conditions of Participation:** CMS should remove the proposed revision to the Medicare and Medicaid hospital Conditions of Participation to require electronic patient event notifications, and instead consider alternative mechanisms for promoting admission, discharge and transfer notifications, such as modifying the measures under the health information exchange objective of the hospital and Critical Access Hospital Promoting Interoperability programs.
- **Information blocking:** HANYS urges ONC and CMS to align the proposed rules for the disclosure of electronic health information with the policies currently established under the Health Insurance Portability and Accountability Act.
    - The definition of EHI should remain confined to the narrow set of data originally defined to assist in providing the best clinical care to patients.
    - HANYS requests ONC limit the definition of EHI to the proposed data classes and elements required for certification under the U.S. Core Data for Interoperability standards, which can be updated over time.
    - HANYS urges that providers not be labeled as other types of actors in any circumstance.

  - We encourage aligning Code of Federal Regulations Part 2 with HIPAA before moving forward with requiring sharing some information when other data elements are withheld.
  - HANYS requests a more realistic timeframe that includes a period of education and non-enforcement.

- **APIs for public health plans and 2015 CEHRT:** We support CMS' proposal to require that public health plans make patient health information (PHI) available electronically through a standardized, open application programming interface and API requirements using Fast Healthcare Interoperability Resources for the new Conditions and Maintenance of Certification. However, we believe patient privacy will require that app developers using the APIs must meet a centralized certification process or be required to obtain a business associate agreement with providers.
- **EHI definition**: ONC has proposed a definition of EHI far beyond what Congress intended under the 21st Century Cures Act. HANYS urges the agency to limit the information in the definition of EHI to the data classes and elements required for certification under the USCDI standards.
- **Patient identification**:
  - ONC should require vendors to share their patient matching rates with providers as part of the Maintenance of Certification;
  - CMS should make claims data available to providers through a FHIR-based API to further patient matching;
  - ONC should support the standardization of some demographic data, particularly applying the U.S. Postal Service standard to the address field; and
  - we support CMS expanding the use of the Medicare ID number and recommend ONC add it to the USCDI.
- **Payment and price information:** HANYS opposes the inclusion of payment and price information within the definition of EHI and believes overregulation in this area could impede emerging private sector efforts to promote price transparency.

MEDICARE AND MEDICAID HOSPITAL CONDITIONS OF PARTICIPATION

CMS proposes to revise the Medicare and Medicaid CoPs to include a provision that would require hospitals — including short-term acute, long-term care, rehabilitation, psychiatric, children's, cancer and Critical Access Hospitals — that currently possess EHR systems with the capacity to generate electronic patient event notifications to do so at the time of an inpatient's ADT to another facility or community provider.

HANYS believes ADT notifications would advance clinically appropriate exchange of information. However, **we believe that ADT notifications as a CoP requirement — with the possible noncompliance penalty of decertification — are unnecessary and inappropriate**. We agree that ADT notifications promote appropriate care transitions and exchange of information across settings. The HIEs in New York state certified by the New York eHealth Collaborative are all required to provide this service. Commonwell and Careqaulity and other

national HIEs are also beginning to provide this service. The use of such notifications is evolving naturally as HIE technology evolves.

Therefore, **HANYS strongly urges the administration to not use CoPs as an incentive for hospitals to include ADT notifications.** This proposal, as written, is overly burdensome and draconian.

The proposal should be defined to ensure those providers already participating in an ADT service are not further burdened, but are deemed compliant with this and other portions of the information-blocking provisions by means of their use of a mature HIE. Alternatively, CMS might consider using the Promoting Interoperability program and the Trusted Exchange Framework and Common Agreement to advance this type of EHI exchange in lieu of using a CoP to require ADT notifications. Since maintaining the technical aspects required of the notification system, such as patient matching and a provider listing, likely require the use of an HIE, the TEFCA framework should detail the specifications and incentives for ADT notifications.

We will discuss patient matching concerns further below, but suffice to say here that moving forward with individual ADT notifications without planning for the underlying patient matching mechanisms required would only make a dangerous situation worse. HANYS supports a coordinated effort to develop a national strategy on patient matching.

Operational Challenges of ADT Notifications
The proposed CoP is not an appropriate mechanism for promoting ADT notification for several additional operational reasons. First, by limiting the proposed standard to hospitals that currently have EHR systems with the capacity to generate patient event notifications, CMS recognizes that not all hospitals have been eligible for programs promoting adoption of EHR systems. CMS further acknowledges that there is no specific ONC certification standard for sending and receiving electronic patient event notifications. HANYS appreciates that CMS has proposed an exception for hospitals without the capacity to send notifications. However, we believe the necessity of the exception demonstrates the inappropriateness of the proposal as a revision of the CoPs.

The CoPs are important requirements that all hospitals must meet to protect patient health and safety and to ensure that high-quality care is provided to *all* patients. HANYS anticipates that many post-acute and behavioral health providers, as well as small and rural Critical Access Hospitals would meet the exception. These are some of the settings where care transitions and care coordination are most significant and it would be counterproductive for only some hospitals to adhere to the CoPs. Further, care coordination goals cannot be met when only some providers participate in the transmission of patient event notifications.

As an alternative to creating a CoP, CMS should work with stakeholders to consider modifying the measures under the Health Information Exchange objective of the Hospital and Critical Access Hospital Promoting Interoperability programs to promote ADT notifications. As is the case with all new PI measures, if CMS makes proposed changes to the PI measure sets to promote the transmission of ADT notifications, we urge the agency to allow appropriate time for vendors to update and test EHR systems (at least 18 to 24 months) with an additional year

for hospitals to train staff and update workflows before the measure would be required for reporting. In addition, ONC should include a national ADT notification infrastructure as a core function under the final version of TEFCA to promote transmission of patient event notifications.

INFORMATION BLOCKING

ONC proposes to define information blocking as a practice that is likely to interfere with, prevent or materially discourage access, exchange or use of EHI. Throughout the rule, by offering hypothetical practices that could implicate this practice, ONC demonstrates the scope and breadth of the information-blocking provision. However, ONC also makes clear that it has not attempted to catalog a full list of all potential types of practices that may raise information-blocking concerns.

We support the intention behind 21st Century Cures Act provisions that promote information sharing and prohibit practices that aim to restrict data by purposefully not sharing patient information. These actions harm the health of the population by impeding patients' and providers' access to treatment information, including during emergent situations when timely access is imperative. Stymying access to patient information also subjects patients to duplicative tests, (i.e., lab work and imaging), creating unnecessary costs and unneeded stress for patients.

Currently, a covered entity is permitted, but not required, to use and disclose PHI, without an individual's authorization, for the following purposes or situations: (1) to the individual (unless required for access or accounting of disclosures); (2) treatment, payment and healthcare operations; (3) opportunity to agree or object; (4) incident to an otherwise permitted use and disclosure; (5) public interest and benefit activities; and (6) limited data set for the purposes of research, public health or healthcare operations. The HIPAA regulations allow covered entities to rely on professional ethics and best judgment in deciding which of these permissive uses and disclosures to make. The HIPAA regulations also emphasize providing the minimum information necessary for the intended purpose of the communication. These are important safeguards in protecting patient privacy, which would be effectively eliminated by the proposed rule.

Conversely, the 21st Century Cures Act prohibits healthcare providers and HIT developers, networks and exchanges from engaging in information blocking, defined by the statute as "a practice by a healthcare provider, HIT developer, health information exchange, or health information network, except as required by law or specified by the Secretary as a reasonable and necessary activity, is likely to interfere with, prevent or materially discourage access, exchange, or use of electronic health information."

HANYS is concerned that any time a hospital declines to provide access to a patient's information in the exercise of professional judgment under HIPAA, it would be accused of information blocking. This proposed rule also places hospitals in an untenable position where state and federal health information privacy laws, or the relevant facts, are unclear: the hospital would have to choose between disclosing the information (and risking a breach) or not disclosing the information (and risking an allegation of information blocking). The proposed exceptions do not provide adequate assurances that hospitals would be protected

from information-blocking claims by the Office of Inspector General for declining to make available certain EHI in a manner that is currently protected under HIPAA. **HANYS urges the agency to align its proposals for the disclosure of EHI with the policies currently established under the HIPAA regulation for mandatory and permissive disclosures by healthcare providers.** Further, any future changes to the HIPAA disclosure requirements that conflict with more restrictive state laws — such as those in New York — would be unduly burdensome.

HANYS appreciates the significant thought that has been devoted to crafting the seven information-blocking exceptions. However, we are concerned that, as proposed, the information-blocking provisions would add significant regulatory burden. This is contrary to the administration's goals to reduce burden on healthcare providers.

Below we offer specific comments related to the proposed definition of EHI, the proposed definitions of regulated actors under the information-blocking statute and proposed information-blocking exceptions. In addition, we urge the agency to consider a significant period of non-enforcement as entities across the healthcare system are educated about and develop compliance procedures and policies on the new requirements.

Definition of electronic health information
The definition of EHI is not specified in the statute. The proposed rule defines EHI as electronic PHI and any other information that is:

- transmitted by or maintained in electronic media;
- identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
- relates to the past, present or future health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual.

HANYS is concerned that this expansive definition of EHI goes beyond Congress' intent of the scope of information required to be shared and conflicts with the permissive use provisions of HIPAA. Additionally, an expansive definition of EHI would unnecessarily complicate implementation of congressional policies to improve communications among providers in caring for their patients, especially across the care continuum, and particularly in light of the very expansive definition of healthcare provider that ONC proposes.

Providers should not be faced with reviewing a significant quantity of information about a patient's past history that is not relevant to the treatment of the patient's current condition. With respect to healthcare providers furnishing clinical care to patients, often on an urgent or emergency basis, the intent of Section 3022 is to make available the pertinent information expeditiously. Thus, the definition of EHI is intended to focus on a narrow set of data that will help providers furnish the best clinical care to patients.

Data under USCDI should define EHI
As part of its updates to certification requirements, ONC proposes to replace the Common Clinical Data Set with the USCDI standard to increase the minimum baseline of data classes commonly available for interoperable exchange. In addition, ONC proposes to establish a predictable, transparent and collaborative process to expand USCDI going forward, including providing stakeholders with the opportunity to comment on the expansion.

HANYS requests ONC limit the definition of EHI to the proposed data classes and elements required for certification under USCDI, which can be updated or expanded upon over time. This definition would provide regulated actors with certainty on which information is required to be shared and ensures that actors are sharing information on an even playing field where all Certified Electronic Health Record Technology captures the required information, reducing regulatory burden for all. If ONC wishes to expand the definition of EHI in the future, it could do so through its proposed process to expand USCDI, with opportunity for a notice and public comment period.

Definitions of actors regulated under the information-blocking statute
The 21st Century Cures Act prohibits information blocking by healthcare providers, HIT developers, networks and exchanges. HIT developers, networks and exchanges are subject to different penalties than providers, which are required to be subject to "appropriate disincentives," which CMS proposes as public reporting of information-blocking attestation statements. ONC proposes to use the very broad definition of healthcare provider established under the HITECH ACT.

Significantly, the agency notes that a healthcare provider could also be operating as a different type of actor — such as a health information network — under certain circumstances. This is because the definition of an HIN under the proposed rule relates to individuals or entities that facilitate exchange of EHI between one or more unaffiliated individuals or entities, which many hospitals and health systems do routinely as part of care coordination efforts. Similarly, ONC provides a definition for HIT developers that acknowledges the role of providers as self-developers of CEHRT. ONC proposes that a self-developer of CEHRT would be treated as a healthcare provider for the purposes of information blocking.

HANYS supports the proposal related to self-developers as it reduces confusion about which information-blocking penalties an individual or entity is subject to. HANYS urges the agency to reverse its position and clarify that if an individual or entity's primary role is as a provider they cannot also be considered a different type of actor for the purposes of information blocking. This revision would be consistent with the statute's requirement that penalties imposed by reason of the information-blocking rules are not duplicative. This nonduplication requirement was intended to apply both to penalties imposed under other provisions of law as well as penalties that may be imposed by OIG under Section 3022 of the Public Health Service Act.

If in addition to serving primarily as a provider, a provider is acting as one of these other three types of actors, the provider should not be subject to the penalties reserved for developers, HIEs and HINs. Subjecting providers to the up to $1 million per information-blocking penalty creates significant risks to the healthcare system. For example, if providers acting in any of these additional capacities are subjected to these civil monetary penalties, there could be

unintended consequences, especially for smaller and mid-sized providers who could deduce that if they would be treated as an HIE they may not be able to withstand a $1 million penalty and would make decisions accordingly. We are concerned that a punitive policy of this nature could also further diminish rural provider access and could unintentionally lead to additional hospital consolidation. Last, we believe this proposal would conflict with the administration's intentions to bolster competition in the HIT marketplace.

Information blocking — public reporting
CMS proposes to publicly report on *Hospital Compare* and *Physician Compare*, respectively, the names of clinicians and hospitals who submit a "no" response to any of the three attestation statements, as an appropriate disincentive under the information-blocking statute.

While HANYS believes that hospitals and clinicians are already financially disincentivized from engaging in information blocking under the Promoting Interoperability program, we do not object to public reporting on the attestation statement responses. However, hospitals and clinicians have reported that under CMS' reporting program systems, any actor that attempts to respond "no" to any attestation statements cannot move forward in reporting additional measures. This may lead to clinicians and hospitals responding "yes" simply to move forward in the reporting system. CMS must address this technical limitation to ensure the data reported are accurate and valid prior to initiating public reporting of the attestation statements.

Information-blocking exceptions
The 21st Century Cures Act directs the Secretary to identify reasonable and necessary activities and practices that do not constitute information blocking. In the proposed rule, ONC identifies seven exceptions that would not implicate information blocking. Each exception is subject to strict conditions that give the actor the burden of proof in demonstrating compliance with the exception.

HANYS appreciates ONC's efforts to identify a thorough list of activities that may interfere with the access, exchange or use of EHI, but are reasonable and necessary under certain circumstances. However, HANYS is concerned about the significant burden placed on hospitals in demonstrating compliance with exception conditions. Each time a requester makes a request that a hospital deems infeasible, the hospital would be required to timely respond and provide a detailed written explanation of its reasons for denial. Hospitals frequently receive infeasible requests, including from patients and their family members, payers, researchers and others. For example, data requests made of hospitals by researchers are more appropriately handled by entities that are charged and qualified to release specific information. Many of these requests do not merit a detailed written explanation of the reason for denial. It is also inappropriate to place the burden to prove a request is infeasible on the provider.

Patient harm
ONC proposes to establish an exception to the information-blocking provision for practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. HANYS supports ONC's proposal for the first exception related to

patient harm. We believe this would help promote information sharing across the care continuum. However, we have some practical concerns.

While ONC acknowledges laws like 42 CFR Part 2 require patient consent before sharing information, ONC also states that the exemption cannot be justified just because a patient did not give consent to share some information such as sensitive data (i.e., Part 2), thus making the record incomplete. Unfortunately, many EHRs cannot segregate sensitive data from other data. HANYS strongly supports aligning Part 2 requirements around sharing sensitive health information with HIPAA rules on less sensitive health information. However, until these policies are aligned and until EHRs are evolved to the point where sensitive data can be easily segmented, providers will experience challenges outside their control related to sharing records containing sensitive health information.

We also do not understand how the information-blocking rule supersedes Part 2 rules.

Last, we are aware that the Substance Abuse and Mental Health Services Administration plans to release new rules around Part 2 shortly. It will be important to review any changes prior to finalizing this exception.

HANYS urges ONC to clarify that instances of emotional harm could be included in the definition of patient harm. For example, clinicians may wish to avoid a situation where a patient learns of a significant diagnosis that would adversely affect the patient's mental state through an electronic transmission of information, prior to a face-to-face encounter where the clinicians can provide important context and information about the care plan that could otherwise put the patient at ease.

Exception #2: Promoting the privacy of EHI
ONC's second exception applies to reasonable and necessary actions that protect the privacy of an individual's EHI, provided certain conditions are met. ONC affirms that any practice to protect the privacy of an individual's EHI must be consistent with applicable laws related to health information privacy, including the HIPAA Privacy Rule as applicable, as well as with other applicable laws and regulations, such as the HITECH Act, 42 CFR Part 2, and state laws. ONC further proposes that an actor would need to satisfy at least one of four proposed sub-exceptions in order to be covered by this exception.

Overall, while we appreciate the detailed approach and intention behind this exception, our members believe exception #2 with the four sub-exceptions is overly complex, and if adopted as proposed, could create unnecessary administrative complexity and burdens. We recommend that providers only be required to meet existing requirements under HIPAA.

Period of education and non-enforcement
As previously mentioned, the 21st Century Cures Act information-blocking provisions represent a significant change in the health information sharing framework for the entire healthcare system. As proposed, the information-blocking provisions would be effective the day of a final rule's publication. However, providers, vendors, health plans, HINs and exchanges need time to understand the new regulations and develop plans for organizational and individual compliance. Such planning requires development of, or modifications to,

policies regarding protection of PHI, as well as substantial staff and patient education. HANYS urges ONC to issue an interim final rule with comment period, and clarify that information-blocking provisions are effective no earlier than 18 months following publication of the interim final rule.

We also ask that ONC and OIG conduct more substantial and in-depth outreach and education efforts for the policies that are finalized. Given the vast array of actors (the proposed definition of healthcare provider alone is very expansive) and differing needs for understanding expectations as they exchange EHI among themselves, patients and other parties in compliance with the information-blocking rule, HANYS believes that a significant period of non-enforcement is required to ensure adequate time for all regulated actors to adapt to and understand what is required for compliance within this new framework. This is especially important given the wide variety of requests a healthcare provider receives.

HANYS urges ONC to approach its disincentive policy in phases. It should begin with a long period of non-enforcement, during which the agencies conduct expanded education and training efforts. ONC and OIG should emphasize corrective action over financial penalties, with the latter being reserved only for actors displaying a pattern of noncompliance or disregard of the information-blocking rule that results in patient harm. The disincentive for actors with a pattern of violations should be tailored to the severity of the violations.

Request for comments on price information

The proposed rule includes a request for comment on the inclusion of price information within the scope of EHI for the purposes of information blocking as well as a series of wide-ranging questions on how best to make price information available to healthcare consumers if it were to be classified as EHI.

HANYS strongly opposes ONC's view that price information can be included within the scope of EHI for the purposes of information blocking. The 21st Century Cures Act was focused on leveraging IT to support patient clinical care. An expansion of the EHI definition to include pricing information not only exceeds the agency's authority but would shift away from clinical uses of health information. Given that there is no existing evidence that the wide-ranging availability of price information could improve patient outcomes or lower consumer and overall health spending, ONC must continue to focus the industry on standardization of health information for clinical care improvement.

HANYS believes that the best price information available to consumers is from their insurers and/or Medicare/Medicaid. Insurers (public and private) negotiate and/or set service prices across networks of providers. As a result, the meaningful price for consumers for health services is only derived once the insurer's negotiated discount is applied or price is set. Therefore, the best source of information regarding prices a consumer will pay is and should remain his or her insurer.

Price transparency efforts should focus on protecting consumers from unexpected and unnecessary out-of-pocket healthcare spending. There is no evidence that the broad-based disclosure of hospital charges or insurer-hospital negotiated prices across a full suite of

hospital services helps consumer decision-making or lowers overall health system costs. Instead, the government and others should focus on initiatives that limit unexpected and unnecessary out-of-pocket spending for consumers. New York's surprise billing/out-of-network law is a national model for protecting consumers from financial exposure for emergency services and our state's hospital financial assistance law protects low-income New Yorkers from hospital bills. Initiatives like these, which have a proven record of making hospital coverage and care more affordable for consumers, should be promoted and encouraged.

To create the most effective price transparency initiatives that help consumers, HANYS suggests that ONC and CMS jointly convene an independent expert panel of multidisciplinary stakeholders to study:

- current initiatives that have protected consumers from excessive out-of-pocket healthcare spending (i.e., out-of-network laws);
- the effect that transparent prices would have on consumer and overall health spending;
- legal questions/concerns on the proprietary nature of negotiated price information;
- how quality data could interact with price data to more fully inform consumers;
- how price and quality data could be best created, structured, formatted and stored;
- what is the best format for consumers to consume price data (EHR, public website, other format); and
- what common definitions could be deployed for healthcare price transparency terminology, including price, charge, cost, etc.

API REQUIREMENTS

CMS proposes to require that public health plans make PHI available electronically through a standardized, open API, which would allow third-party applications to electronically access the information. Specifically, the requirement would apply to Medicare Advantage organizations, Medicaid state agencies, state CHIP agencies, Medicaid managed care plans, CHIP managed care entities and Qualified Health Plan issuers in federally facilitated exchanges. The information made available through an API would have to include patient claims and encounter data, provider directory data, clinical data (including lab data) held by the organization and drug benefit data, including pharmacy directory and formulary data. ONC has also proposed revisions to the 2015 Certification Criteria for EHR vendors to include the use of standardized APIs for patient and population services.

The most significant issue with the use of open APIs in the manner described above is the privacy and security of PHI in the hands of non HIPAA-covered vendors. **HANYS urges CMS to consider taking steps to address privacy concerns prior to requiring the release of PHI to third-party applications.**

Since the passage of HIPAA in 1996, patients have understood that their health information will be kept confidential. However, commercial application companies generally are not HIPAA-covered entities. Therefore, when information flows from a hospital's or health plan's information system to a third-party application, it likely no longer would be protected by HIPAA. Most individuals would not be aware of this change and may be surprised when commercial application companies share health information obtained from a hospital or health plan, such as diagnoses, medications or test results in ways that are not allowed by HIPAA. Furthermore, individuals may consider the hospital or health plan to be responsible if their data are sold to a third party or used for marketing or other purposes.

While we agree with CMS that empowering patients through consumer-directed exchange is integral to engaging patients in their care and advancing healthcare transformation, we also share the concerns of others that consumers may not be fully aware of the implications of such exchange. **Most consumers have a general sense that their PHI is afforded certain protections, but are not aware that when authorizing access to a third-party application not associated with their provider or payer, their PHI is no longer protected by the privacy and security protections under HIPAA.**

We support the provisions CMS proposes to require payers subject to this requirement to post educational materials such as those made available by HHS and we encourage HHS to further explore efforts to more broadly ensure consumers are meaningfully informed prior to authorizing a third-party application access and use of their PHI. Similarly, we urge CMS to maintain the proposed provisions that allow for denial or discontinuation of access by third-party applications when it is reasonably determined the application would pose an unacceptable security risk to the PHI maintained by the payers, including state Medicaid programs.

The concerns above leave providers with no means to ensure that vendors have gone through a systematic process to validate an app from a security or privacy standpoint. While some big vendors appear to be doing a good job of interfacing with the large technology companies in the app management ecosystem space, this is not yet a widespread practice, nor is it mandatory.

Our members are also concerned that some apps/third parties may take patient data and use it in ways not known to patients, as we have seen with some large technology companies. We fully agree patients have a right to their data; nonetheless, the news coming out daily around inappropriate use of consumer data offers ample evidence that patients are very much at risk of having their health data used in ways they never intended or authorized.

HANYS urges CMS to work with stakeholders to establish an industry-backed, third-party vetting process for applications that would give patients confidence that their health information is secure, while being clear when HIPAA protections no longer apply. In addition, we believe there is much to be done in the area of healthcare consumer and privacy literacy. In the event this is deemed too burdensome or may hinder desired timelines, the vendors providing third-party apps should be required to sign business associate agreements.

Request for information on sharing information between payers and providers through APIs

In the proposed rule, CMS notes that payers and providers may seek to coordinate care and share information on an overlapping patient population in a single transaction. CMS seeks comment for future possible rulemaking on allowing a provider to access or download information from a payer on a shared patient population through an open API. HANYS supports the development of a future proposal that would allow providers to access more information from payers on shared patient populations. Our members' experience is that when information is shared under risk and value-based arrangements, there are improvements in care coordination and management of the total cost of care. We look forward to working with the agency on specifics of these proposals.

PROVIDER DIGITAL CONTACT INFORMATION

The 21st Century Cures Act emphasizes the importance of making provider digital contact information available through a common directory. The CMS proposed rule would increase the number of clinicians with valid and current digital contact information available through the National Plan and Provider Enumeration System. NPPES has also added a public API, which can be used to obtain contact information stored in the database. CMS proposes to publicly identify those clinicians who have not submitted digital contact information in NPPES.

Providers are currently struggling with multiple directories and would welcome a single source of digital contact information. However, there are several concerns with the directory plan as proposed.

CMS notes that many providers have not yet submitted digital contact information and what is listed is frequently out of date. To increase participation, CMS proposes to publicly report the names and NPIs of providers that do not have digital contact information stored in the NPPES beginning in the second half of 2020. HANYS is concerned that CMS is placing much of the burden for collecting this information on providers, rather than the agency, as Congress intended. We urge the agency to better educate providers on the availability of the new digital contact fields on the NPPES. Further, CMS must give providers adequate time to familiarize themselves with the availability of these fields. CMS must also take steps to ensure the contact information is accurate and up to date.

We do not oppose public reporting of providers that have not updated the NPPES with their digital contact information, but appropriate notification to the provider in advance of public reporting, with appropriate time to make corrections and updates, would be a valuable tool for ensuring the most complete information. Additional reminders for updates and other agency efforts to ensure the database contains reliable and valid information is imperative; otherwise, the data collection effort is moot.

UPDATING THE 2015 EDITION CERTIFICATION CRITERIA

ONC proposes a number of updates to the 2015 Edition Certification Criteria, including adoption of a standardized approach to open APIs by requiring the use of the FHIR standard. ONC also proposes to expand the set of data classes and constituent data elements to be shared by naming the USCDI Version 1 as a standard. HANYS generally supports this proposal and believes it would result in a more streamlined transfer of health information.

HANYS urges ONC to consider comments from stakeholders, in particular from HIT developers, on the appropriate timeline to implement these changes — generally 18 to 24 months following publication of a final rule. Providers must be given at least one additional year to upgrade their CEHRT. As noted previously, HANYS also supports ONC following a predictable, transparent and collaborative process to expand UCSDI.

Privacy-related criteria changes
ONC proposes to update the Data Segmentation for Privacy (DS4P) 2015 Edition certification criteria. Currently, certified HIT models must support privacy tagging of EHI at the document level only. The new criteria, though still based on the C-CDA and the HL7 DS4P standard, must enable tagging at the document, section and element levels. ONC proposes another new certification criterion, "consent management for APIs," to facilitate data segmentation involving APIs. Modules would be required to align with the open source Consent2Share API *Implementation Guide*, designed to work with FHIR standards for APIs. The new DS4P and consent management criteria would become effective with the subsequent ONC final rule. It is our understanding that data segmentation tagging will be a feature of FHIR Release 4, but ONC's proposal is to move to Release 2, so we are unclear how this would work. It is also our understanding that neither Release 2 nor DS4P are backwards-compatible and do not have as many resources as Release 4.

HANYS has concerns about the privacy-related criteria requirements and their implementation timeline. ONC notes that uptake of the current, simpler, DS4P standards has been minimal so far. More granular privacy tagging and consent management APIs potentially could improve exchange of EHI subject to special handling (e.g., related to behavioral health or child abuse). However, modules drilling down to the element level would be more complex and costly to develop than the current criteria, with costs being pushed downstream to users.

Further, the putative benefits of granular tagging (e.g., eliminating workarounds to satisfy specific state regulations) may not be fully realizable without increased conformity among federal and state privacy provisions. Finally, we note that ONC identifies some ambiguity as to which FHIR release versions are, in fact, supported by the Consent2Share *Implementation Guide*.

HANYS encourages ONC to consider deferring adoption of the DS4P standards and consent management criteria at least until an API FHIR standard version is finalized and the Consent2Share guide is revised to conform to that version. The additional time could be used for testing strategies to mitigate our members' concerns about unintended privacy consequences that might arise when patients unknowingly allow redirection of their EHI to others through third-party APIs that may not be HIPAA-compliant. Ideally, the privacy related criteria would be delayed until ONC has deemed the FHIR Release 4 as the new standard.

Privacy and security transparency attestation
ONC has proposed to add two new 2015 Edition privacy and security "transparency attestation" certification criteria: Encrypt authentication credentials and multi-factor authentication. ONC is calling for vendors to attest that they either do or do not have this capability. Vendors, however, would not be required to have this functionality even though it is currently inexpensive and ubiquitous. CHIME is not aware of any reasonable justification for

making encryption an optional part of certification and other expert entities have called for such a requirement.

Late last year, the public-private Joint Cybersecurity Workgroup published *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, 13*, which recommends encryption. This workgroup clearly cited the lack of encryption as a vulnerability. And the Health Care Industry Cybersecurity Task Force report issued in June 2017 makes several recommendations to improve EHR security, including requiring strong authentication to improve identity and access management for healthcare workers, patients and medical devices/EHRs. The report recommends that "In situations where the provider is accessing an EHR or Health Information Exchange external to the hospital or clinical environment, the health care industry should adopt the NIST SP 800-46 guidelines for remote access including the use of two-factor authentication to ensure a compromised password cannot alone be used to gain access." Having the capability to do single sign-on would remove several administrative burdens for clinicians.

HANYS recommends that ONC require vendors to offer encryption and multi-factor authentication, as well as single sign-on capabilities, to all their clients under their certification requirements, rather than just having to attest that they do or do not offer these features.

CONDITIONS OF CERTIFICATION AND MAINTENANCE OF CERTIFICATION

Developer gag clause removal
ONC proposes a new Communications Condition of Certification that would not allow HIT developers to restrict or prohibit ("gag") communication among users of their modules about a module's real-world function and the developer's support of the module. Developers would be required to notify all customers within six months of the effective date of ONC's subsequent final rule that any existing "gag clause" contract provision would not be enforced by the HIT developer. Only a few exceptions to the gag clause prohibition would be permitted.

HANYS supports the proposed Communications Condition and customer notification deadline. Our member hospitals often informally share important information with each other to advance patient care (e.g., emerging antibiotic resistance patterns, care coordination strategies). However, our members have been precluded from similar sharing about their HIT module experiences by their contracts with HIT developers. Gag clauses can delay the identification of module features through unintended consequences, such as interfering with clinical workflow, impeding care coordination and presenting potential patient safety threats. HANYS applauds ONC for the thoughtful approach to this topic. Providers have long been plagued by gag clauses and some have repeatedly been prohibited through contracts to share information like screen shots, even if it was related to patient safety.

Patient matching RFI
The ONC and CMS proposed rules include complementary requests for information regarding patient matching. We are delighted to see the administration focusing on such a critical issue. The ability to uniquely connect a patient to his or her medical record is paramount for both interoperability and patient safety reasons.

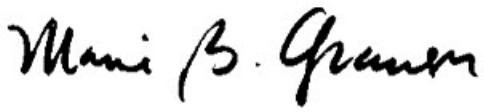
We note that the term "patient matching" is often used interchangeably with "patient identification," but these terms have distinct meanings. Patient identification is the ability to uniquely and accurately match a patient to his or her record. Patient matching may be defined as the linking of one patient's data within and across healthcare providers to obtain a comprehensive and longitudinal view of that patient's healthcare. Patient matching involves using referential and matching algorithms to link accounts from two separate systems. Without accurately connecting a patient to his or her data, patient safety and interoperability issues would persist.

Best practice guidelines should be created to include the use of a standardized process for patient identification and capturing patient information no matter where registration occurs. We encourage CMS to continue exploring the possibility of expanding the use of the Medicare ID to improve patient matching. CMS should work with ONC to ensure that vendors, as part of their Maintenance of Certification, are required to share their patient matching rates and other related information. These data could be used to improve and standardize patient matching algorithms. If a biometric is ultimately adopted, it must work in a variety of healthcare settings. CMS should make claims data readily available in a timely manner to providers through a FHIR-based API; doing so would help providers better match patients.

HANYS and all our member institutions appreciate your attention to these details that affect all of our originations and patients. We look forward to working together to improve care and increase data availability while reducing burdensome documentation and regulations.

If you have questions, please contact Thomas Hallisey, director, health information technology, at (518) 431-7719 or thallise@hanys.org.

Sincerely,



Marie B. Grause, RN, JD
President