

HHS Proposes Steps Toward Health Data Interoperability

CMS and ONC Proposals Would Implement Cures Act

Stephen Barlas

It has been 10 years since Congress passed the HITECH Act, which, together with the \$36 billion in grants from the Recovery Act, spurred the computerization of hospitals and physician offices with the goal of making electronic health records (EHRs) simple to create, easy to share among providers, and simple for patients to access. That was the promise. Today the reality is something quite different.

Announcing its latest effort to breathe life into that 10-year old dream, the Centers for Medicare and Medicaid Services (CMS), which released a parallel proposed rule to the one issued by the Office of the National Coordinator for Health Information Technology (ONC), stated on March 3: “Despite the fact that 78 percent of physicians and 96 percent of hospitals now use a certified EHR system, progress on system-wide data sharing has been limited.”

The verdict may be even worse than that, however. Besides making digital records portable and health care thus more effective, the billions of dollars spent were meant to save time and ultimately money for providers, especially physicians and programs such as Medicare and Medicaid. That hasn’t happened, for the most part. At the Senate Health, Education, Labor, and Pensions (HELP) Committee hearings on March 26, Senator Lamar Alexander (R-TN), committee chairman, commenced by talking about a Tennessee physician who would have to spend \$26,000 a month to have his printed patient records digitally converted—by a hospital visible from his office window. His EHR system is incompatible with the hospital’s EHR system. “So, for Dr. Blackwelder and many other physicians, recordkeeping is more expensive and burdensome as a result of electronic health-care records,” Alexander said.

The Trump administration, like the Obama administration before it, is in the midst of a number of rulemakings, all with the same objective: improving the information encoded in EHRs, making it easy to share among providers, and collecting it in one place so patients can easily access what they need to stay abreast of their health issues and provide a complete health record to new providers and insurers. The separate but allied proposed rules from CMS and ONC implement provisions in the 2016 21st Century Cures Act that are primarily meant to force federal health-plan providers to make data available via cell phone to plan members, encourage EHR software suppliers to adhere to expanded but voluntary certification standards, and jettison some proprietary features of competing systems that have prevented systems from communicating with one another.

Medicare’s proposal supports CMS’ initiative MyHealthEData, and follows on their 2018 regulations allowing potential payment

reductions for hospitals and clinicians. This is to encourage providers to improve patient access to EHRs by using standardized application programming interfaces (APIs). In Medicare’s fee-for-service program, CMS launched the Blue Button 2.0 API, which enables its beneficiaries to access their health claims information. “CMS currently has over 1,500 application developers building tools with this API,” say Kyle Gregory and Paulette Thomas, attorneys at BakerHostetler who specialize in health-care technology issues.

For the first time, CMS is now proposing that Medicaid, the Children’s Health Insurance Program (CHIP), Medicare Advantage plans, and Qualified Health Plans (QHPs) on the federally facilitated exchanges provide enrollees with immediate electronic access to medical claims and other health information via APIs by 2020.

How those records will be provided is ONC’s part of the equation. Its proposed rule focuses on technologies that will make it easier for health care apps to obtain patient information. The information available to patients through APIs will be based on new ONC software-certification requirements. Those, in turn, will be based on the Health Level Seven’s (HL7[®]) Fast Healthcare Interoperability Resources (FHIR[®]) standards. Developers will then have to make products that conform to those standards in order to get ONC certification, which is voluntary (but in some sense mandatory) for software companies wishing to sell to federal health programs and their suppliers.

However, Ben Moscovitch, the project director of health information technology at the Pew Charitable Trusts, explained to the Senate HELP Committee, “FHIR permits the depiction of data elements in different ways and considers the inclusion of some data as optional, which could inhibit interoperability. To reduce this variability, ONC proposes to require the use of an implementation guide developed by the Argonaut Project—a collaboration between technology developers and health care providers—that provides constraints on how to implement FHIR.”

Pharmacy Implications

“Overall, the proposed rules appear to focus more on patients having access to their own health care data and less on actual interoperability,” states Rebecca Chater, RPh, FAPhA, director of clinical healthcare strategy at Omnicell. “With that said, the EHR certification and mandate to go to HL7 FHIR should help both patients and pharmacies gain easier access to a patient’s medical records.”

As they do not participate in Medicare incentive programs such as Promoting Interoperability (formerly Meaningful Use), retail pharmacies will not be directly affected by any final rule. But there are larger reasons why they should take note. Shelly Spiro, executive director at Pharmacy HIT Collaborative,



Stephen Barlas

Mr. Barlas is a freelance writer in Washington, D.C., who covers issues inside the Beltway. Send ideas for topics and your comments to sbarlas@verizon.net.

HHS Proposes Steps Toward Health Data Interoperability

notes that just as pharmacies adopted e-prescribing, they will have to adopt open APIs and send data, especially to health plans based on the FHIR standard and particularly if they want to expand their business beyond drug prescriptions to more clinical-care functions. There are very few pharmacies, retail or inpatient, with FHIR capability now, and not many who can report via the less comprehensive Pharmacist eCare Plan. “If we can’t see where we need to be, we’ll never get there,” states Spiro.

Hospitals will be under the gun when the rules are finalized, and that carries implications for inpatient pharmacies. For example, ONC’s new certification standard for EHRs would include a new e-prescription standard: the National Council’s Prescription Drug Program (NCPDP) SCRIPT version 2017071. This would be equivalent to CMS’ requirement for the Part D e-prescription and medical history effective January 1, 2020. The new standard is also likely to be injected into other Medicare programs, such as the Query of Prescription Drug Monitoring Program (PDMP) measure in the Physician Fee Schedule and Hospital Inpatient Prospective Payment System. However, there are some timing issues relating to when the new SCRIPT standard becomes an exclusive requirement in Medicare prescribing and the older SCRIPT 10.6 (in ONC’s 2015 Edition Health IT Certification Criteria (2015 Edition) is no longer eligible. When they publish their final rules, CMS and ONC will decide on timing.

The certified APIs will be based on an expanded data set called the U.S. Core Data for Interoperability (USCDI), replacing the Common Clinical Data Set (CCDS) specified in ONC’s 2015 Edition. Among the new elements that will have to be included in the USCDI are information on the author of physician notes, the author’s organization, and a time stamp for data elements in the EHR. The inclusion of provenance will allow patients and clinicians to understand whether a medication was entered by a primary care physician or at a hospital. The time stamp will allow apps to chart or sort information, by listing patient medications starting with the most recent, for example.

Uncertainties Abound, Including Over Implementation Costs

A lot about CMS–ONC’s combined effort seems speculative. In a blog post, Don Rucker, MD, the national coordinator for Health Information Technology, conceded somewhat paradoxically, “While we do not know exactly what a secure open API future will bring, we can expect change in health care to be transformative.”

Recently, Paul Black, Chief Executive Officer of Allscripts, who has extensive experience with EHRs, wrote the following: “The rules are broad, and they are very assertive in the topics explored and the timelines proposed—possibly, I think, exhorting more than Congress intended in some cases.” Allscripts claims it was the first in the industry to offer open API access to its EHRs. Those APIs have enabled almost 6.5 billion data-exchange transactions.

But Black worries that “a requirement to license nearly every solution—a concept that seems [to be] an abrogation of normal patent protections—would effectively penalize those investing in technology evolution. When coupled with the proposed cost recovery exception, which would undermine free-market pricing

influences and essentially limit profit opportunities, the proposals in this area seem to discourage innovative investment.”

Are software developers going to spend money on certification? And what will it cost their customers? ONC estimates that the proposed rule’s final cost for the first year (including one-time costs) would range from \$365 million to \$919 million, with an average cost of \$642 million. After the first year, annual costs are projected to range from \$228 million to \$452 million, with an average cost of \$340 million. The first year “benefit” would average \$6.1 billion, and \$5.8 billion each year thereafter.

Concetta Rasiarmos, a spokeswoman for Allscripts, says, “Allscripts offers our APIs for no additional license or maintenance fee. There are one-time service fees associated with implementing and configuring FHIR APIs within the client’s EHR, and we also offer a premier package for clients who want help with their own internal API-based development projects.”

The CMS Proposed Rule

The key requirement CMS is proposing is that Medicaid and CHIP fee-for-service programs, Medicare Advantage programs, and QHPs make a variety of information accessible to patients via “openly published” APIs; thus, that technical and other information required by third-party apps to connect to APIs would be publicly available. Data subject to that mandate would be the elements in the USCDI standard: information on enrollee claims, encounter data, utilization history, and clinical health.

Theoretically, these APIs will allow patients to access their health data on their phones. But CMS does not require health care providers such as hospitals, who already report data to federal health programs, to make that data available to other providers a patient might be using: in other words, there is no larger interoperability requirement. CMS had considered the following alternatives for mandating this requirement in its proposed rule for the 2019 inpatient hospital-payment program:

- Participating in, or serving as, a health information network that is part of the Trusted Exchange Framework and Common Agreement (TEFCA);
- Maintaining an open API that allows persistent access to third parties, which enables patients to access their health information; and
- Participating in the piloting and testing of new standards that support emerging interoperability use cases.

The agency declined to endorse any of them for this year, but will reconsider the matter when proposing inpatient payment changes for 2020. Meanwhile, CMS is advancing a proposal to expand the Conditions of Participation (CoP) to require hospitals, psychiatric hospitals, and critical access hospitals (CAHs) to make electronic patient event notifications available to another health care facility or community provider. The requirement is limited to facilities currently possessing EHR systems that can generate information for these notifications. The notices would need to be sent at the time of a patient’s admission then either immediately prior to or at the time of discharge, or transferred to a list of post-discharge providers who meet certain qualifications.

Even that narrow requirement is likely to raise hospital opposition. The American Hospital Association (AHA), respond-

HHS Proposes Steps Toward Health Data Interoperability

ing to a Medicare request for information published as part of the proposed hospital inpatient payment changes for 2019, stated: “We do not believe a new mandate tied to CoP is the right mechanism to advance health information exchange. Instead, the AHA urges CMS to focus its attention on resolving problems created by the lack of a fully implemented exchange framework, adoption of common standards, and incentives for EHR and other IT vendors to adhere to standards.”

Christopher R. Rehm, MD, chief medical informatics officer at Lifepoint Health, told the HELP committee in March, “While I support this idea directionally—and look forward to achieving this level of information-sharing—this is unfortunately putting the cart before the horse. It sounds like it would be simple to implement, but there are numerous unanswered questions and operational considerations. For example, not all EHRs can generate these messages—and this functionality isn’t required of vendors under the ONC certification.”

The ONC Proposed Rule

A crucial provision in the 21st Century Cures Act was one authorizing ONC to end information blocking by health information technology (IT) developers, hospitals, and health care networks, who may not want rivals to have access to some of their data for competitive reasons. However, Lucia Savage, chief privacy and regulatory officer at Omada Health and former chief privacy officer at ONC, told the HELP committee, “The 21st Century Cures Act applies the prohibition against information blocking to developers of ‘health information technology’ as defined in HITECH Section 13101(5). The ONC proposal, however, applies only to a subset of this category, certified EHR developers. This limitation leaves out many types of health IT where individuals’ health facts are collected. For example, the proposed rule doesn’t reach to health IT in the emerging world of connected devices or Software as a Medical Device, and seems to omit any non-certified EHR, such as a lab or pharmacy electronic-records system that is not certified.”

Although ONC strives to stop information blocking, it does allow seven proposed exceptions to the mandate, which are intended to protect patient safety and promote the privacy and security of electronic health information. According to ONC, these exceptions would allow for the recovery of costs reasonably incurred; excuse an actor from responding to infeasible requests; and permit the licensing of interoperability elements on reasonable and non-discriminatory terms. Another exception addresses activities that are reasonable and necessary to promote the performance of health IT.

It remains to be seen how disruptive, or not, these exceptions will be in a new world with no information blocking. Another potential threat to seamless EHR software communication is ONC’s scaled-back self-certification standards. In 2017, ONC reduced the overall burden for testing health IT by confining testing to the 2015 Edition rules, changing 30 test procedures to attestation only. The agency’s proposed March 2019 rule lists six further deregulatory actions.

These include eliminating some of the “policing” requirements for ONC-Authorized Certification Bodies (ONC-ACBs), which until now have only been required to proactively surveil two percent of the certificates they issue annually. That would be modified to suggest that ONC-ACBs *may* conduct

in-the-field, randomized surveillance. The two-percent floor would be eliminated. The certification bodies would still have to perform reactive surveillance when they receive specific complaints, and they would be permitted to conduct their own randomized surveillance.

And what happens if a developer whose system doesn’t qualify for an exemption nonetheless includes features that support information blocking? What penalties exist? In the proposed rule, CMS states that it would “publicly report the names of clinicians and hospitals who submit a ‘no’ response to certain attestation statements related to the prevention of information blocking...” Also, ONC would share information with the Office of the Inspector General (OIG), who could investigate claims of false attestation. Typically, OIG refers allegations of Medicare or Medicaid fraud to the Department of Justice for potential prosecution.

However, “there remains a considerable amount of ambiguity around information blocking, even with the exceptions laid out in the proposed rules, making it difficult to tell how ONC and OIG will handle review and enforcement,” explain Gregory and Thomas.

Don’t expect the major EHR software developers to embrace ONC’s proposal wholeheartedly. “We are committed to openness, transparency, and fairness as principles of interoperability,” says Anamarie Rebori Simmons, spokeswoman for Cerner. “We continue to support the goal of the proposed ONC rule to create broader, streamlined access to electronic health information for legitimate purposes under prevailing law, and are focused on expanding our open, standards-based APIs.” But Cerner’s support of the “goal”—and not necessarily the elements of the proposed rule—coupled with its preference for “prevailing law” seem to indicate that the company will not happily wrap both arms around ONC’s proposal.

Epic also supports the “goals” of the two proposed rules, according to a company spokeswoman, but “there should be more clarity around different types of data elements and how the information-blocking provision applies to each.”

Health Care Data Privacy

Even if standardized open APIs are universally available, interoperability, in its gold-standard form, may be impeded by shortcomings in patient identification. The best way to overcome that is to assign each patient a unique patient identifier (UPI). But Congress has forbidden CMS and ONC to explore the possibility of developing UPIs in case of privacy-protection shortcomings. Instead, ONC has fallen back on a less satisfactory strategy called “patient matching,” where health information from various sources is compared to identify common elements, with the goal of identifying records that represent a single patient. This is generally done by using multiple demographic data points such as name, birth date, gender, and address.

The rules proposed by ONC and CMS, if finalized as they are without further dilution, will undoubtedly give the broader health care system a kick in the pants on the road to interoperability. But that kick will land the system only halfway up the road, a fact that CMS admits, acknowledging “the limits of our authority to require use of APIs to address our goals for interoperability and data access...” ■