Testimony for Senate Committee on
Health, Education, Labor and Pensions

Hearing March 26, 2019

Implementing the 21st Century Cures Act: Making Electronic Health Information Available to Patients and Providers

Christopher Rehm, MD

Chief Medical Informatics Officer

LifePoint Health

Chairman Alexander, Ranking Member Murray, and Members of the Senate HELP Committee, thank you for the opportunity to testify before you today. It is an honor to be invited to participate in today's discussion.

My name is Christopher Rehm. I am a physician and the Chief Medical Informatics Officer at LifePoint Health. LifePoint Health is a provider organization that delivers Acute, Emergency, Post-Acute and Outpatient care for over 85 communities in 30 states. Our clinical technology environment consists of 10 different Inpatient electronic health records (EHRs), greater than 10 Ambulatory EHRs, and countless vendor partners providing departmental, ancillary and point solutions. My team and I work with our hospitals and providers to build, configure and tie together these systems so that our providers are set up for success to provide safe, efficient, high quality care to each and every patient we see in the communities we serve.

The desire to make electronic health information freely available spans the political spectrum and has been a long-standing goal of patients and those who care for them. These proposed rules represent an important step in our journey to achieve the ultimate aims of a truly person-centric health care delivery system. I applaud this committee and federal health agencies for recognizing the need to improve existing regulations to keep pace with evolving technologies and innovations. I support the ability of patients to have access to their health information and understand that the future health of our population and the sustainability of our industry depends upon the timely, efficient movement of data.

There are several ways that we can choose to navigate toward this future state. The new Centers for Medicare & Medicaid Services (CMS) and Office of the National Coordinator for Health Information Technology (ONC) rules represent the interpretation of the great work that this Committee did on the 21st Century Cures Act. And we support the general direction of the rules. Having said that, if we do not take time to consider how these new rules may affect certain stakeholders in the health care ecosystem, especially providers and patients, the decisions that we make today may have unintended consequences for years to come.

Cost and Regulatory Burden of Health IT on Providers

I am here today as a health care provider – someone who has taken care of patients and oversees others who take care of patients. I love my work because there is no other place or profession where people are so consistently caring and devoted to alleviating human suffering caused by disease. But many of the forces facing hospitals, doctors, nurses and patients make it really hard to do the job well.

Some of the most stifling forces are those imposed by our technology and the regulatory policies that govern them. Electronic medical records, devices, diagnostics, monitors—these are all things that are supposed to augment our practice, to help us be better caregivers. Instead, our technology only adds to the complexity and burden that we feel. Part of the problem is that there is no underpinning that supports a system-of-systems for technology in the health care industry. No one has established the rules of the road for data exchange, like industries such as banking, aviation, cable, telecom and others did decades ago. Vendors develop products and services that do not interoperate. In order to support some level of communication across systems, the market has created even more products and services—like integration and interface engines—that help to glue together these proprietary technologies. But it is up to the providers to bear the burden and cost of implementing and integrating all of these separate pieces, and it doesn't stop once we have bought them.

Many vendors release products that meet minimum viability standards for ONC certified technology, but their service contracts do not include the cost of maintaining and updating them to remain compliant with new regulations. Coming into compliance with new or updated regulations generally involves upgrading the EHR or device to modify how information is documented, collected and reported.[1] The average-sized community hospital (161 beds) spends nearly $760,000 annually on information technology investments needed to support compliance with federal regulations.[2] These IT changes and associated costs are crushing our industry where margins are already thin.

Additionally, these upgrades take time. Six months is simply not enough time for a provider organization to review, build, configure, test, train and deploy numerous vendor technologies following new releases to be ready to meet the regulatory deadlines for reporting under the CMS programs. IT product design, testing and implementation requires lead time, particularly when it involves a vendor. Timeframes for implementation and updates need to be adjusted to reflect what is reasonable and acceptable, for instance, 12 months after a Generally Available release date from a vendor.

We applaud the ONC proposal to require health IT vendors to demonstrate that their products are usable to patients and providers in a real-world environment. Any solution can work in a vacuum. We need our health care technology and software systems to work in real life settings and in concert with many other vendor technologies if we expect them to meet the needs of patients and providers now and in the future.

[1] Assessing the Regulatory Burden on Health Systems, Hospitals and Post-acute Care Providers. *American Hospital Association.* February 2018.

[2] Assessing the Regulatory Burden on Health Systems, Hospitals and Post-acute Care Providers. *American Hospital Association.* February 2018.

While the HITECH Act catalyzed the move from paper to digital records via incentives and penalties on health care providers, it did not, unfortunately, address or create an underlying infrastructure of interoperability to enable data liquidity among technologies. Think about this for moment: it is the equivalent of telling people they must buy cars and move those cars from place to place, but there are no roads and no agreed upon design for the roads, let alone the funding to actually pay for the construction. In the case of EHRs, it is the provider organizations who have been left to bridge the gap with everything from integration and interface engines, to workarounds that lead to significant "clicks" for clinicians, to even a combination of electronic and manual processes.

Health care providers are trying hard to persist in their dedication, but the increasing pressure of having to do more with less weighs heavily on these well-meaning people. Atul Gawande's November 2018 article was aptly titled "Why Doctors Hate Their Computers,"[3] and a joint Fortune and Kaiser Health News article just last week highlighted and astounding average of 4,000 clicks per shift for an emergency room doctor.[4] Clinicians need our support, encouragement, and appreciation for the value they bring to patients and to society.

As a health care provider, I support the ability of patients to have access to their health information and the sharing of information across disparate technologies, systems, and providers. The CMS proposed rule would require, as part of the Medicare Conditions of Participation (CoPs), hospitals to send electronic notifications when a patient is admitted, discharged, or transferred. Hospitals would be required to send these notifications to other facilities, providers, or community care providers with an established patient relationship who the hospital has reasonable certainty will receive the notifications. 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 is not required of vendors under the ONC certification

[3] Atul Gawande, *Why Doctors Hate Their Computers*, The New Yorker (Nov. 12, 2018), https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers.
[4] Erika Fry and Fred Schulte, *Death by a Thousand Clicks: Where Electronic Health Records Went Wrong*, Fortune and Kaiser Health News (Mar. 18, 2019), http://fortune.com/longform/medical-records/.

rules. And if a provider is not connected to a health information exchange or similar network, of which the most advanced ones are quite costly, it is an enormous undertaking – in both time and money – to connect to these other providers and facilities individually.

In order to comply with a CoP, providers must clearly understand what it is they must do and how they will be surveyed and judged to determine compliance. This proposal lacks both of those elements, which is concerning given the tremendous penalties hospitals face for failing to comply with CoPs, including termination from the Medicare program. Instead, I encourage the Administration to focus on its current activities to improve interoperability, such as continuing to advance the goals of the Trusted Exchange Framework and Common Agreement (TEFCA), as well as its proposals in this rule to further ensure vendors are accountable for the products they develop. The responsibility for interoperability cannot and should not be borne solely by providers, and there are plenty of things that vendors, business associates, plans and other organizations can and should be expected to do and contribute.

Patient Privacy and Security

It is clear that Congress and this Administration are committed to solving the issue of interoperability and achieving complete patient access in the U.S. health care system. So far, the Administration is relying on third party apps and the private market to solve these problems. The rules state that they wish to "enable patients to access their health information electronically …to make the data available through an application programming interface [API] to which third party software applications connect to make the data available to patients."[5]

Providing unvetted third party applications fairly open access to patient digital health data concerns me as both a clinician and a consumer. I am well-aware of the argument that it is the patient's prerogative to specify where and to whom their data goes. Personally, I like the idea of controlling my own data. But reality does not always align with our ideas, particularly when it comes to our personal information – whether health-related, financial, or even demographic. The truth is that the vast majority of us, myself included, do not read the entire "terms of use"

[5] 84 Fed. Reg. 7610, 7612 (Mar. 4, 2019).

agreement on every app or website that has some of our personal information, and we often mistakenly believe our data is more private or more secure than it actually is.

While it may be tempting to allow access to personal digital health information for any and all entities who claim to operate under the banner of "promoting care coordination," we would be wise to take a lesson from the consumer data privacy events of the past few years. Millions of individuals were surprised and angry to learn how Facebook was using and selling their data, while other consumers weren't even aware that all their financial information is funneled through three to four major credit bureaus, two of which experienced major breaches in the last few years.

Digital data is the currency of the modern technology ecosystem and marketplace. There are fortunes to be made in mining and monetizing your personal digital health data. New rules and processes that govern and protect digital health data must be sensitive to the reality that not all covered entities, business associates, and third parties are created equal. Particularly with regard to entities that fall outside of the HIPAA requirements, it is imperative that patients, their families, providers, and consumers can trust that these applications – and the data both sent to and received from them – are secure, private, and clinically sound.

The vision for the future is one in which a patient's data flows between her/his care providers, the patient and her/his providers, and between the patient's personal electronic device and the provider.
That vision presupposes that data is vetted, clinically sound and comes from a trusted source. The reality is that neither clinicians nor patients have the ability to validate that it is trusted data.

A Trust-Based Approach

I believe there are ways to support the innovation coming from the external marketplace while providing the needed safeguards to govern personal digital health data. The entrance of non-health care actors into the health care market – particularly those that fall outside of the HIPAA requirements – necessitates strong principles for trust and security. One such idea is an industry-backed trust platform technology architecture, supported by an appropriate governance model.

This is a wide-ranging solution that would encompass all health-related digital information on a single platform architecture. In the meantime, I also encourage a smaller scale solution to address privacy, security, and clinical efficacy of third-party applications, specifically an industry-backed process to independently vet these applications to ensure they are meeting all relevant security standards; are using data appropriately and in line with consumer expectations; and, for those applications that offer medical advice, are clinically sound. Such a process will go a long way towards ensuring trust while removing the burden of this process from consumers and providers.

What Federal Policy Can Do

Policymakers must strike a balance between their desire to make personal digital health information available and the burdens that these requirements place on health systems under proposed timelines. Government policies must allow digital health information to be exchanged in a way that protects and prioritizes the interests of individuals – and the health systems and clinicians who care for them – while allowing the marketplace to innovate and interact in a responsible and controlled way.

In this technological age, it is important we all remember that the deployment of health information technology, interoperability, data exchange, privacy and security are all in service of patients receiving and providers delivering the safest, highest quality care. It is not about the technology; it is about patients, their care, and their outcomes.