ONC'S INTEROPERABILITY RULE – RISKS AND SOLUTIONS
December 2019

1. PRIVACY EXPOSURE FOR FAMILY MEMBERS – WORSE THAN FACEBOOK

It seems good to let patients direct health systems to send their data to whatever apps they choose. However, most app vendors are not HIPAA-regulated and studies have found that the majority of mobile health apps re-sell or share the data. Throughout the patient record there may be information about family members. Once the patient clicks "I accept" the information may be mined without the family members' knowledge and used in unanticipated ways that family members and health systems would consider unethical. Facebook and Cambridge Analytica demonstrated how friends' personal information could be commercialized and exploited in shocking ways. This is worse because it is health data. Health systems may find themselves facing class action lawsuits.

ONC has said this is justified because 1) patients currently enter health data into apps, and 2) patients share their genomic profiles with companies such as 23 & Me. However, patients entering health data into mobile apps usually don't enter private information about family members. And knowing a person's genetic profile doesn't mean you know that her brother, a prominent businessperson, has an addiction. This will open up a whole industry where the data is sold to tabloids, employers, opposition researchers, marketers, etc.

It would take too long for health systejms to read each patient's record and eliminate all reference to family members. Similarly, technology does not exist for EHR developers to locate family member references.

Solution: Delay the final rule until Congress passes appropriate privacy legislation.

2. SCOPE – TOO VAST, TOO BURDENSOME, TOO DANGEROUS

A patient's medical record contains several thousand data elements (medications, lab results, etc.) which are standardized (defined so everyone can understand the meaning) and exchanged electronically. The essential set of standardized data is called USCDI (or U.S. Core Data for Interoperability). The rest of the health system data consists of about 160,000 data elements (such as doctor's workstation, time patient's room cleaned). Most of these data elements help the health system operate, are not standardized, and exchanging them means huge effort with minimal value because there are no shared definitions.

Transmitting non-USCDI data in order to comply with the rule requires a tremendous amount of work for the health systems and the EHR developers with little benefit to the patient. It will take EHR developers approximately 320,000 hours (for 160,000 non-USCDI data elements) to evaluate what to include, audit the decision, develop the code to package up the data, test it, etc. Then health systems will have to take thousands of hours to evaluate their own additional data elements, questionnaires, specialized flow charts, etc. The penalty for getting this wrong can be up to $1M per infraction.

The rule says that a health system does not have to disclose de-identified data of its population but oddly does not similarly protect Limited Data Sets, which contain more patient information than de-identified data. Bad actors can demand LDS from a health system under the same terms the health system has shared the LDS with others, and the health system cannot decline without legal justification.

If EHR developers and health systems are swamped with requests and cannot respond quickly enough to be within the brief timeframe allowed, they may be liable for the up to $1M per incident penalty. Health systems will have less time for patient care and EHR vendors will have little time left for EHR continued development and innovation.

Solution: Limit the scope of the rule to USCDI. Expand the definition of USCDI to include relevant pricing information and to grow as needed over time. Allow health systems to choose what organizations they allow to get a Limited Data Set. Allow health systems and EHR developers to determine a responsible maximum number of requests per day. Significantly reduce the $1M per incident penalty and do not penalize entities making good faith efforts.

3. THEFT OF INTELLECTUAL PROPERTY – CYBER THREATS, LOSS OF AMERICAN COMPETITIVENESS

The rule removes trade secret protection that EHR developers have used for decades to safeguard their intellectual property. Screens depicting workflows, processes, and, algorithms can no longer be protected. EHR developers must revise every contract accordingly. Many of these components of intellectual property have taken thousands of people many years to create. EHR developers that have succeeded over the years have done so because they have developed software and engineered workflows that others have not been able to develop. Now the rule takes their intellectual property away, disallows protection of screen designs, removes longstanding contractual rights to defend intellectual property, and in essence gives their know-how to those who have not been able to compete on their own. This rule enables the theft of EHR developers' intellectual property.

Foreign companies, especially in tech savvy countries such as China and Russia, will be able to reverse engineer the software, greatly undermining the competitiveness of American health IT companies, especially internationally. (The Indian company Tata stole Epic's trade secrets. Epic won the lawsuit; Tata is appealing the amount of damages awarded.)

Motivated attackers, understanding in detail how the software works, could launch targeted malware and cyber-security attacks – changing blood types, altering IV volumes – endangering lives of patients and putting health systems into crisis.

Solution: Intellectual property is the underpinning of American innovation and should remain fully protected.

4. MARKET CONTROL – GOVERNMENT CONSCRIPTION VIOLATES AMERICAN FREE MARKET PRINCIPLES

The rule essentially conscripts EHR developers to become software engineers for market entrants, even dictating the fees the developers may charge. Although the stated goal is improving patients' access to their data, the rule subjugates EHR developers and takes away their work and their rights. A product or algorithm may have taken software developers and data scientists years to create and involved hundreds of trips around the country and the world to get it right. An EHR developer may have invested tens of millions of dollars to create the product or algorithm. The rule requires EHR developers to offer their work to any new vendor at the miniscule cost of the transfer of the information, divided by the number of vendors that want it. This will chill innovation among EHR developers. It is excessive regulation that goes against American free market principles.

Solution: USCDI standards-based data should go from one health system to another for the care of the patient at no charge. Patients should be able to receive their own USCDI data electronically at no charge. For non-USCDI data, EHR developers should be able to decide how to license their technology and should be able to set their own terms and prices. Government should support free market principles that the country has been built on, and should not set prices.

We have shared these concerns with HHS and ONC staff and leadership and they may be working on changes to some parts of the rule. Many others (health systems, healthcare associations, patient privacy advocacy groups, EHR vendors, and government agencies) have also shared their concerns.