September 4, 2020

Dr. Donald Rucker
National Coordinator
Office of the National Coordinator for Health Information Technology
330 C Street, SW
Floor 7, Switzer Building
Washington, DC 20024

RE: ONC Patient Identity and Patient Record Matching

Dear Dr. Rucker,

Congress’s initial intent for patient privacy and data security developed when digital information was locked into a single electronic health record (EHR) and the Congress thought of care as a transaction between a patient and clinician during a single point of contact. We now know an individual patient is treated across a care continuum by several clinicians and different systems where data sharing are essential to coordinate, optimize care, prevent harm, and reduce costs. However, current law prevents the federal government from spending federal dollars toward the adoption of a universal patient identifier (UPI) solution for patient matching. Patient information is kept locked away and makes true data sharing for optimal care unattainable. The ACS strongly believes the development of a UPI or a mechanism that allows for accurate and reliable patient matching is necessary. In an ideal state, patients should have the option to ensure the safe management and exchange of their data in a secure and private manner. Therefore, we support a legislative fix to remove Section 510 from the Labor-HHS appropriations bill to give HHS the ability to consider the best nationwide strategy for patient identity solutions.

Without a UPI, the industry is forced to use work-around methods to match patient data. Inaccurate patient matching can lead to adverse events, compromised safety and privacy, or inappropriate and unnecessary care. These workarounds are intended to correct any misidentification but are an unnecessary burden on both patients and physicians because they are time consuming and place expensive burden on health systems. Errors in individual data matching will be compounded with the expansion of digital health information sharing required as part of the 21st Century Cures Act.
The COVID-19 pandemic has revealed the impact and exponential complexity of this problem. The lack of a UPI hinders accurate patient tracking and matching across every aspect of managing the pandemic—including testing, therapeutic treatment, vaccine deployment (if/when a vaccine becomes available), and longitudinal tracking of long-term impacts of the disease, to name a few. Understanding the impact of COVID-19 requires shared knowledge for individual patients as well as for the population as a whole. It would be prohibitive to create a scalable patient identifier to track patients in a fast-changing pandemic.

In the absence of a UPI, many of the work-around solutions put patient privacy at greater risk by requiring patients to disclose individually identifiable information for multilevel authentication of their identity. First level workaround solutions call for patients to reveal their social security number, birthdate, address, credit information and other personal demographic information. Second level authentications consider web-based information and past ownership history such as previous addresses, phone numbers, color of vehicles or previously held loans. The more complex the workarounds, the more the certainty of a patient’s identity approaches the effectiveness of a UPI. However, these workarounds fail to achieve the level of reliability and validity as a UPI while exposing and putting at risk much more of a patient’s identity. This seems contradictory to the overall intent of protecting patients’ privacy.

Ideal State: UPI

The development of a patient identity solution, such as a UPI, would allow patient information to move between clinicians, patients, and payers in a secure and private manner, while also guaranteeing that the correct data are being exchanged for the correct patient. With a UPI we would be able to achieve an ideal state with the ability to aggregate knowledge about a patient across the lifespan of a patient’s condition(s) and clinical encounters, allowing us to track a patient longitudinally with predictive analytics that support machine learning and artificial intelligence. This is important if we want to get out of the business of transaction-based care and simple clinical data registry reporting where patient data is held in silos. A UPI is the most secure and efficient way to get to predictive analytics that will allow clinicians to get in front of a disease and anticipate sequela and risk, rather than responding to it. For example, this level of knowledge management can allow for predictive diabetes care. For surgeons this may mean having the ability to identify a cohort of diabetes patients with a higher risk of adverse outcomes for a given procedure, and know what is needed to decrease patient risk through enhanced care pathways pre-operatively or postoperatively. When clinicians are able to realize the potential to assemble knowledge and expose critical information
with a high level of reliability made possible by a UPI, healthcare will undoubtedly be transformed. The benefits and opportunities associated with these types of predictive analytics are endless.

**Interim UPI Alternatives**

In the absence of a legislative fix for this issue, the ACS recommends that ONC continue to explore alternative solutions. From the regulatory perspective, we suggest the ONC collaborate with other federal agencies to develop solutions to achieve safe and reliable patient matching to enable longitudinal management of patient information. With today’s technological capabilities there are various opportunities for improvement in current patient matching practices. For example, solutions that utilize block-chain technology, biometrics, or technologies currently offered by private vendors that store, manage, and track identifiable information—similar to practices used in the credit card industry—could be incorporated in alternative patient matching solutions. The ACS is very supportive of the work ONC has done on this issue and encourages the agency to continue engaging stakeholders, private sector technology vendors, healthcare providers, and the other federal and state agencies to develop a safe and effective solution for identifying and matching patients to their health information.

In the below sections, we discuss specific alternatives that ONC should consider as they explore patient matching and identification solutions. As part of this discussion, it is important to note that, while many health systems and insurance providers have already taken steps to better identify patients and match their health records within their internal systems by using demographic information and internal identification numbers, these systems have shortfalls. They run patient’s information through internal matching algorithms, but many of these algorithms are not easily scaled, are exclusive to the specific organization, and do not ensure a 100% positive matching rate. The utilization of these systems is moving us in the right direction, but there are many limitations and challenges that require health systems to expend extensive resources and also put patients’ sensitive health information at risk.

**Vendor-supported Solutions**

Much of the problem with verifying a person’s identity comes from lack of access to enough unique data to ensure the match is truly accurate—when only using demographic information collected from the patient there is great risk for misidentification. ACS encourages ONC to explore opportunities that allow health systems and providers to connect to secure databases that store individual’s digital identities in larger data sets. These databases could include
past phone numbers, name changes related to major life events, credit cards, and more, which allow providers to verify patients’ identities with increased accuracy.

While this could allow for a larger number of accurate matches, there are obvious challenges with utilizing these digital databases as the primary solution to support patient matching. Databases that manage large amounts of identifiable information are owned privately—therefore hospitals will be required to expend extra financial resources for these services, and they are limited to matching individuals who have digital identities. Additionally, when using these systems, there are still barriers to accurately matching children (since they do not have a digital footprint) and those who choose to avoid sharing their information digitally. In addition, health systems may need to employ staff to verify certain matches where the probability of the match isn’t significant.

There are other technologies that ONC may consider that are built on the same foundation, but go one step further, where the collection of the data and the establishment of the identity is patient-directed. In the trusted relationship between the health system and the identity management system, the onus to establish and maintain the identity is on the company providing the service. To ensure positive identity matches for individuals, the patient would need to willingly share certain information such as demographics, but combine that information with a biometric variable, such as a fingerprinting or facial recognition. Using biometric scans would ensure that the system is not creating duplicate records of a single person. While this reduces some risk of inaccurate patient matching, there may still be some level of inaccuracy for certain populations, such as children, identical twins, those who endured severe burns or trauma that have altered their appearance, or individuals who do not want to be identified.

Overall, alternatives that use broader identity management databases are more scalable than the approaches used in health systems today. But there are still many questions about how health systems would share patient identities and how identities verified by different organizations would be matched correctly. Without a UPI, will patient identities ultimately come from a single identity database and require a federally regulatory action to mandate a standardized methodology? For example, if many of the large health systems contracted with their own identification vendors that developed positive matches within their system, the patient could be easily identified when visiting any provider within that system. But should the patient visit a clinician who uses a separate proprietary identification system, a crosswalk would need to be developed between the two systems so patient information can be easily queried and
matched to maintain a longitudinal health record and avoid duplication of records. The U.S. healthcare system has faced similar challenges in the context of achieving interoperability among electronic health records, which the federal government, in consultation with industry stakeholders, has aimed to address through the use of mandated standards and unified criteria. A similar standardized approach is needed to ensure accurate and consistent patient identification protocols. Without a UPI, patient identification processes will continue to be disjointed and will add considerable cost and complexity to the overall care of a patient.

**Blockchain Solutions: Self-sovereign ID**

Blockchain technologies are being used to securely identify individuals in many industries such as banking. Many believe that these technologies could help solve the patient matching and identification issues in healthcare. For example, a blockchain-like solution such as a self-sovereign identity (SSID) allows patients to create, own and control their own digital identities. SSIDs also allow patients the ability to consent to who accesses their health record, and the components of the health record that are shared.

For example, a patient could create an SSID, is given a digital key, and can save the SSID in their own digital wallet along with their other SSID’s. But they can also share the SSID with a health information exchange (HIE) to save in its ledger (blockchain), as shown in the visual below. The HIE would be responsible for verifying the patient’s identity and encrypting and notarizing it to ensure it is matched to the proper patient and used for its intended purpose. Through the SSID, the patient can digitally sign a consent-to-share form with the digital key associated with their SSID to allow the HIE to share their records with its community. This consent would then be saved in a computable format within the HIE’s blockchain to be used to determine what information can be shared with certain clinicians each time a query is made for the patient’s record. Clinicians or healthcare systems who participate in the HIE would query the HIE for the patient records as needed, and the HIE would decrypt the patients consent, determine if the patient has opted to share their record with the querying clinician, and if so, the clinician can then retrieve the requested documentation.
Because the patient also has control over this SSID, they can edit or delete their consent to share forms at any time, which could be done easily through applications on a smartphone. Another element of the SSID is the patient’s ability to have more granular control of the information in their health record. This means that within the patient’s consent form they can determine which domains (psychiatric, substance abuse, infectious diseases, etc.) they do or do not want shared with certain clinicians. Within a patient’s consent form, a patient could, for example, specify that they only want their psychiatric data to be shared with psychiatrists, so if their record was requested by their surgeon the HIE would remove the psychiatric data from the record that is shared with the surgeon, and the surgeon is notified that the record had been edited in compliance with the patient’s consent to share form.

This example, where the SSID is shared with the HIE, allows for patient’s information to be shared widely with participants in the designated exchange, but this can also be used in settings outside an HIE. The patient’s record could be accessed via the SSID by healthcare providers outside the HIE, such as dentists, mental health professionals, private insurers, pharmacists, etc., but this would require the patient to complete consent to share forms for each provider, and every new provider they visit in the future. Transitioning to a system where patients play a greater role in how their health records are shared will require increased patient engagement and education.
While the ACS believes that leveraging this technology would be an extremely progressive step in the right direction towards a solution for patient matching, there are also some barriers and challenges that are important to consider. This solution relies heavily on the patient’s ability to determine what information is necessary for their physician to administer treatment. Because patients are not clinically trained, they may not know all the data that are required for physicians to make care decisions, which may lead to gaps in the patient’s records. This may require physicians to spend more time engaging patients to ensure they can access all the necessary information to make safe treatment decisions. We must also consider ways to accommodate and engage special populations, such as older adults who may not be as accustomed to using technology in this way, and those who do not have easy access to smart phones or high-functioning internet services, such as rural and low-income individuals.

In addition to the creation of a patient identity/matching solution, we urge ONC to work with Congress and other Federal agencies, such as the FDA, Office for Civil Rights (OCR), and the Office of the Inspector General (OIG) to more broadly re-evaluate current policies and enforcement mechanisms that oversee today’s privacy and security standards. Current regulations need to be updated to ensure patient data are not shared unless the patient explicitly authorizes it and to limit the extent to which direct-to-consumer and other non-HIPAA covered entities can use and share patient data.

The ACS appreciates the opportunity to provide feedback on these topics for discussion and looks forward to continuing dialogue with the ONC on these important issues. If you have any questions about our comments, please contact Jill Sage, Quality Affairs Manager, at jsage@facs.org.

Sincerely,

David B. Hoyt, MD, FACS
Executive Director