A Unique Patient Identifier Will Benefit Patients While Respecting Their Privacy

Opponents of a Unique Patient Identifier (UPI) raise various privacy concerns with the creation of a UPI, asserting that a UPI would result in a centralized national health records system, that it would allow hackers and foreign governments to steal patient identities, and that it would result in research on identifiable patient information without their consent. **We wholeheartedly disagree with this assessment. Instead, the creation of a UPI would benefit patients and make it *easier* to provide greater autonomy over the sharing of their information.**

UPI and Patient Privacy

- A UPI is not synonymous with a centralized national health records system, and the creation of such a system would not be needed to benefit from having a UPI. Rather, a UPI would further support the current *federated*[1] model of health information exchange by making it easier to match patients across disparate health systems.
- As with any type of patient identifying information that is currently maintained in electronic health records, such as Social Security Numbers, health insurance ID numbers, patient contact information, and genetic data, health care providers will be required to ensure the security of the UPI within their electronic health records, and implement safeguards to prevent hackers and other actors from using a UPI maliciously. Creating a UPI does not change these requirements, or jeopardize the security of the underlying patient information.
- Under HIPAA, Covered Entities and Business Associates may not conduct research on protected health information without first obtaining a patient's authorization, or obtaining waiver of the requirement to obtain a HIPAA authorization from an Institutional Review Board (IRB) or privacy board if the research meets certain requirements. Creating a UPI will not change this.

The Benefit of a UPI for Patient Privacy

- The creation of a UPI should be considered separately from the policy debate about whether health care providers should be permitted or required to exchange full patient records for treatment purposes without patient consent. **If jurisdictions want to limit the sharing of sensitive information across health information exchanges, however, a UPI would make it easier to obtain and to communicate patient privacy preferences for sharing PHI.**
- Currently, "consent management" is difficult in a federated network because it is almost impossible to match with certainty a request for health information about a particular patient with a consent that is stored elsewhere on the federated network. A UPI would make it easier for a patient consent obtained in one context to be applied in other contexts, making it possible to segment data in a patient record based on patient preferences.
- With the ability to perform *distributed* analytics, the need to create large data stores of identifiable data is reduced or eliminated. Instead, queries for relevant data could be run across *locally-managed* data stores, and de-identified data shared in accordance with existing privacy laws.

Success of the UPI for Medicare Beneficiaries

- In MACRA, Congress called for a unique patient identifier for the Medicare population. CMS rolled out new Medicare cards with Medicare Beneficiary Identifiers that replaced the Social Security Number on Medicare cards. Over 61 million Medicare beneficiaries received the new cards in the mail since April 2018.
- While inclusion of the Medicare Beneficiary Identifier is not required to be included with fee-for-service Medicare claims until January 1, 2020, already 86% of fee-for-service claims submitted this year include the Medicare Beneficiary Identifier.

Alternative Approaches that Would Standardize Patient Matching Would Also Benefit Patients

- Should legislators determine that accurately identifying patients to their data is an important public policy objective but have concerns about a UPI, Congress could remove the funding ban and direct HHS to work with the private sector to examine the full array of methods for patient matching, and select and implement a specific, standardized method for patient identification within a specified timeframe.

[1] In a federated model of health information exchange, also known as a decentralized or distributed model, all data stays at the point of service and is shared *only* upon appropriate request. A Record Locator Service can be used to facilitate exchange but the RLS holds only the locators of where authorized health information resides, it does not hold the actual health information data. By contrast, in a centralized model of health information exchange, all data is stored only in a single warehouse or data repository.