



# APIs - Why They Matter

Enabling HIPAA Right of Access

+

Key to Interoperability

=

Patient Safety

## National HIPAA Summit

March 4, 2020

Bettina Experton, M.D., M.P.H.

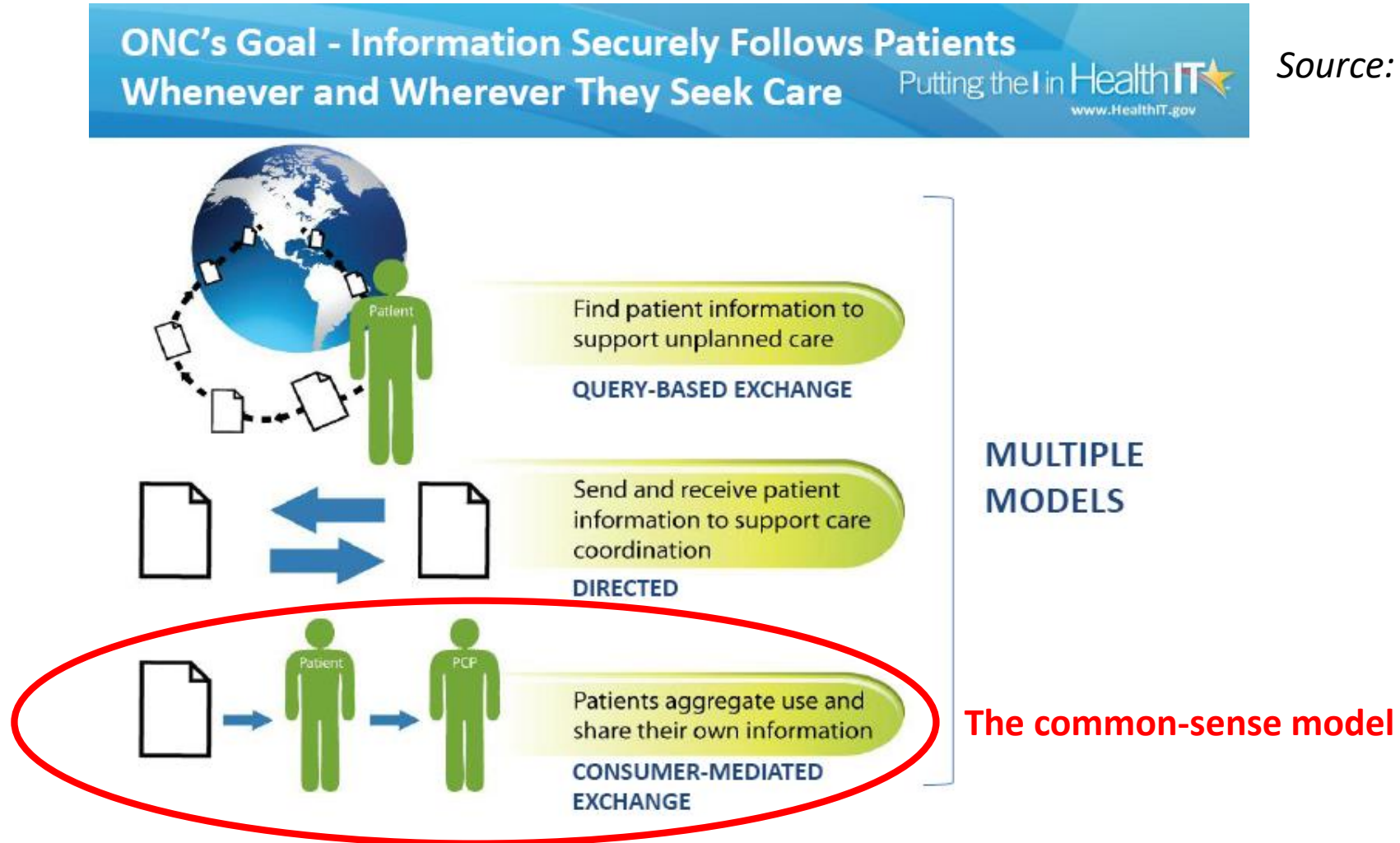
@BettinaExperton

## APIs Practically Enable Individuals' Right of Access

- **Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524** is about “Providing individuals with easy access to their health information to empower them to be more in control of decisions regarding their health and well-being.”
- **With the use of an API-enabled app of their choice, individuals** requesting and accessing their health information can **exercise their “Right of Access”** pursuant to the *HIPAA privacy rule*, and “**without special effort**” under the *ONC interoperability proposed rule*.
- **Without use of standard based API-enabled apps of an individual's choice, individuals are left with no practical means to exercise their Right of Access:** forced to use to multiple portals or provider/payer specific apps, with the inability to consolidate their information in one place.

# Why Are Open APIs Needed to Deliver Interoperability?

- To enable Consumer-Mediated Exchange because Provider-Directed Exchange Never Scaled



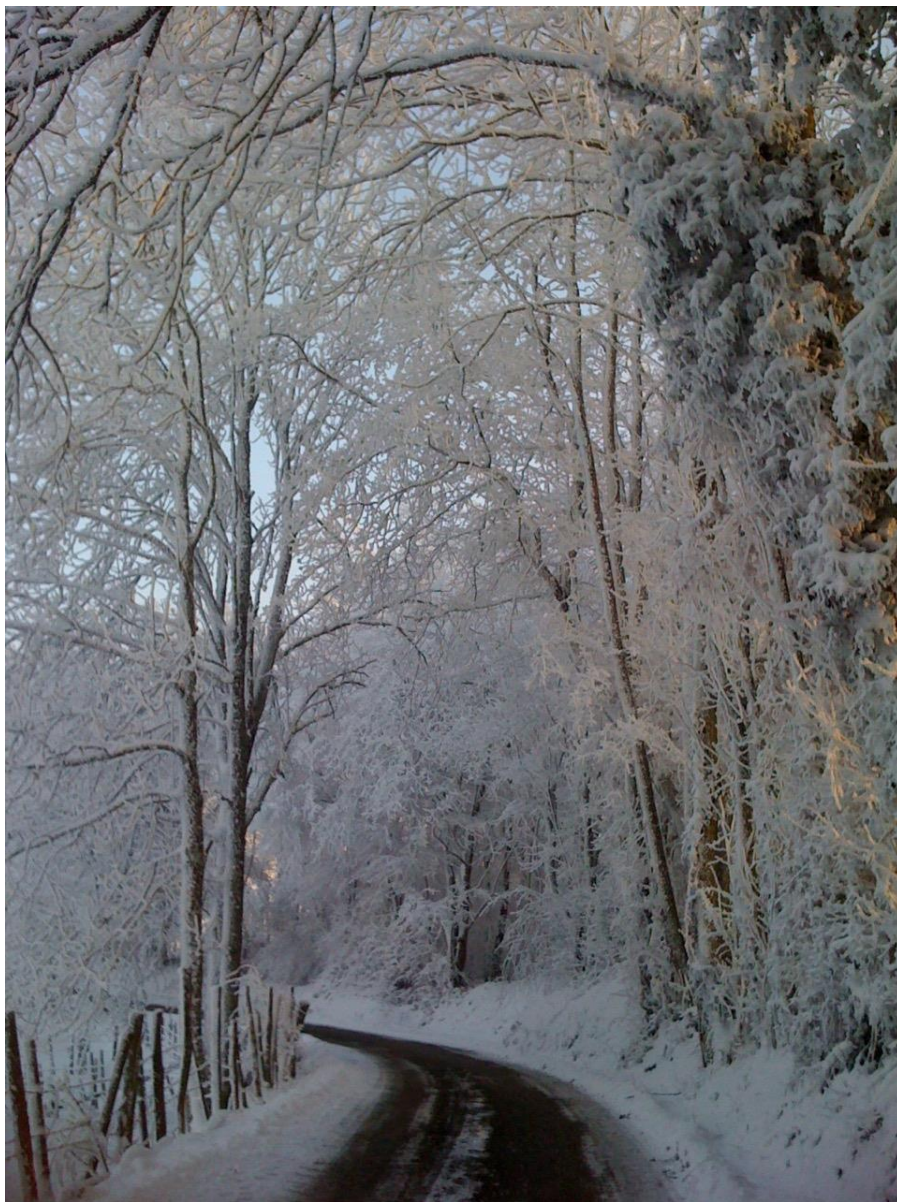
## Consumer – Mediated Exchange: the Common-Sense Model



If there is “Information Blocking”  
on the provider side...

*why not give patients access and  
use of their own data for them to  
use and share with their providers?*





*“It is our patients who  
will lead us out of this  
wilderness”*

Joseph Schneider, M.D., M.B.A  
Former CMIO, Baylor Health Care System, and  
Chair, Council on Clinical Information Technology,  
American Academy of Pediatrics

# Standardized APIs Are at the Core of HHS Proposed Rules for Patient Access and Interoperability

In response to the 21<sup>st</sup> Century Cures Act to cure *Information Blocking*, HHS published on March 4, 2019:

- the **CMS *Interoperability & Patient Access Proposed Rule***,
- the **ONC *21<sup>st</sup> Century Cure Act Interoperability Proposed Rule***.

Both **require either health plans or providers to make use of standards-based open HL7 FHIR APIs** for patient to access their health information at no cost and with their smartphone application of choice.

# The ONC Proposed Rule Is Designed to Give Patients and Providers Access with the Adoption of Standardized APIs



**21ST CENTURY CURES ACT:  
INTEROPERABILITY, INFORMATION BLOCKING, AND  
THE ONC HEALTH IT CERTIFICATION PROGRAM PROPOSED RULE**

## **Application Programming Interfaces (APIs) Certification Criterion and Associated Conditions**



To implement the 21<sup>st</sup> Century Cures Act and improve interoperability, the ONC Certification Requirements of its NPRM calls on HIT developers to:

- Publish **APIs to allow health information to be accessed, exchanged and used without special effort**
- Abide to new EHR **API certification requirements**.
















## ONC Certification Criteria for APIs Address Data Format, Access Authentication and Authorization

- The use of the **Health Level 7 HL7® FHIR® standard** along with a set of implementation specifications that would provide known technical requirements against which app developers and other innovative services can be built.
- **APIs providing patients electronic access to their EHI (including physician clinical notes) at no cost and with their application of choice.**
- **Secure connections that include authentication and authorization** capabilities in ways that enable, for example, patients to use an app to access their EHI without needing to log-in each time they use the app.



# U.S. Core Data For Interoperability: USCDI

## Moving Beyond the Common Clinical Data Set

USCDI v1		
Assessment and Plan of Treatment 	Laboratory  <ul style="list-style-type: none"> <li>• Tests</li> <li>• Values/Results</li> </ul>	Provenance *NEW  <ul style="list-style-type: none"> <li>• Author</li> <li>• Author Time Stamp</li> <li>• Author Organization</li> </ul>
Care Team Members 	Medications  <ul style="list-style-type: none"> <li>• Medications</li> <li>• Medication Allergies</li> </ul>	Smoking Status 
Clinical Notes *NEW  <ul style="list-style-type: none"> <li>• Consultation Note</li> <li>• Discharge Summary Note</li> <li>• History &amp; Physical</li> <li>• Imaging Narrative</li> <li>• Laboratory Report Narrative</li> <li>• Pathology Report Narrative</li> <li>• Procedure Note</li> <li>• Progress Note</li> </ul>	Patient Demographics  <ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> <li>• Previous Name</li> <li>• Middle Name (including middle initial)</li> <li>• Suffix</li> <li>• Birth Sex</li> <li>• Date of Birth</li> <li>• Race</li> <li>• Ethnicity</li> <li>• Preferred Language</li> <li>• Address *NEW</li> <li>• Phone Number *NEW</li> </ul>	Unique Device Identifier(s) for a Patient's Implantable Device(s) 
Goals  <ul style="list-style-type: none"> <li>• Patient Goals</li> </ul>	Problems 	Vital Signs  <ul style="list-style-type: none"> <li>• Diastolic Blood Pressure</li> <li>• Systolic Blood Pressure</li> <li>• Body Height</li> <li>• Body Weight</li> <li>• Heart Rate</li> <li>• Respiratory rate</li> <li>• Body Temperature</li> <li>• Pulse oximetry</li> <li>• Inhaled oxygen concentration</li> <li>• Pediatric Vital Signs *NEW <ul style="list-style-type: none"> <li>- BMI percentile per age and sex for youth 2-20</li> <li>- Weight for age per length and sex</li> <li>- Occipital-frontal circumference for children &gt;3 years old</li> </ul> </li> </ul>
Health Concerns 	Procedures 	
Immunizations 		

# ONC Proposed Rule API Certification Criterion

## API Requirements:

- Certified APIs would need to use the **OAuth 2.0** security standard, widely used in industry
- APIs would need to be able to establish a secure and trusted connection with apps that request data
- **App registration required**
- **Barrier-free registration process** - no longer than five business days - to first verify the authenticity of the developer associated with an app seeking to be registered.
- Approved apps to be registered and **enabled within one business day** of completing developer verification
- **And more likely to come....**

## Security:

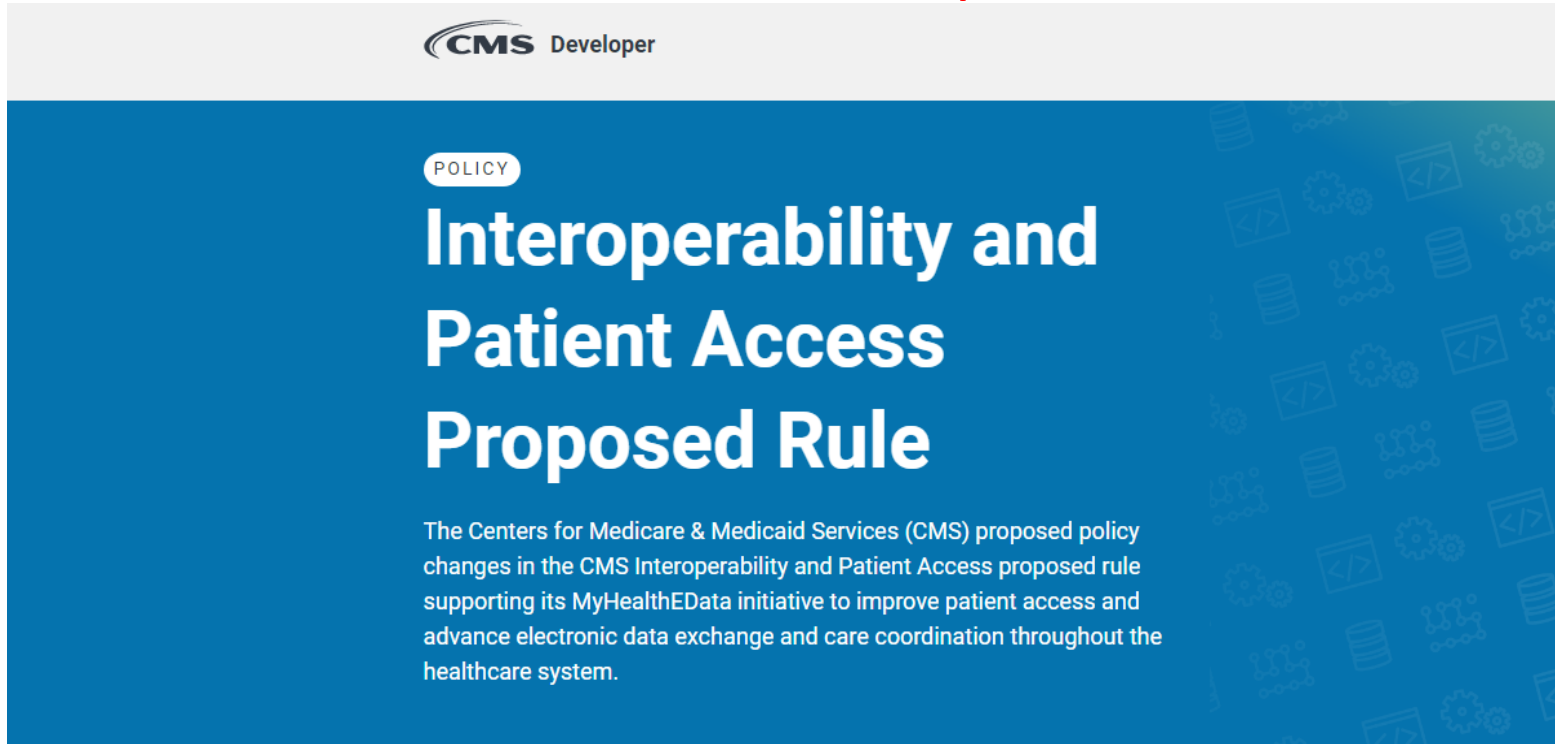
*“Patients complete the authentication process directly with their health care provider, no app will have access to their specific credentials.”*

## Privacy:

*“Patients will be able to limit the data they authorize their apps to access.”*



# The CMS Proposed Rule Gives Patients Access to Their Claim Data with the Adoption of Standardized APIs

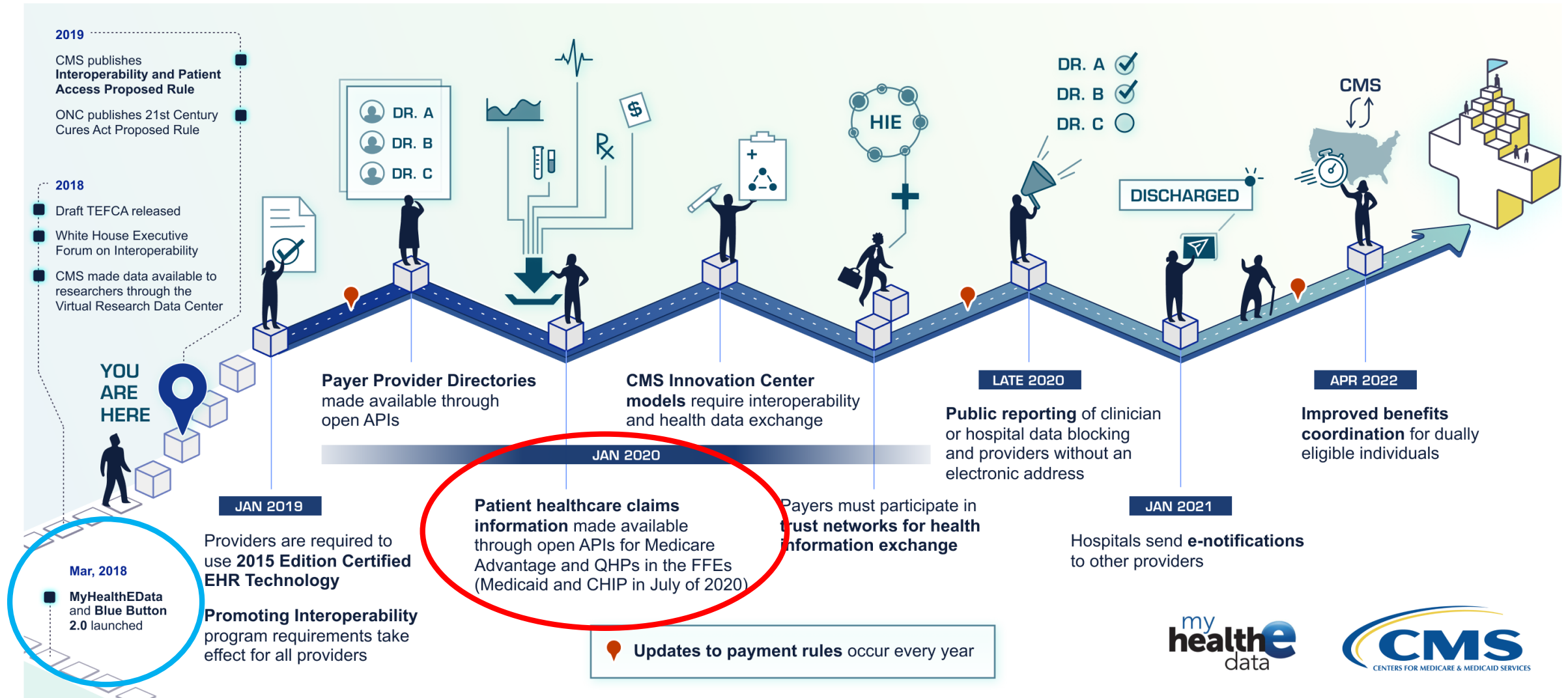


*Patient Access Through APIs*  
empowers patients by ensuring access and use of their healthcare data while keeping it safe and secure.

Having timely electronic access to health information makes it easier for people to make more informed decisions about their healthcare needs.

**Similar to the CMS' Blue Button 2.0 program, Medicare Advantage (MA) organizations, state Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and QHP issuers in FFEs will be required to implement openly-published HL7® based APIs to make patient claims and other health information available to patients through third-party applications and developers.**

# The CMS Proposed Rule Will Give Medicare Advantage Plan Enrollees Access to Their Claim Data with an API-Enabled App of Their Choice, as All Medicare FFS Beneficiaries Can Do Today with a Blue Button App





# Opposing Forces to Open APIs Invoke the Privacy Risk – is This Real?



## **Epic CEO sends letter urging hospitals to oppose HHS data-sharing rule**

Epic CEO Judy Faulkner wrote an email to CEOs and presidents of hospital systems urging them to oppose rules the Department of Health and Human Services proposed in 2019.

Source: [www.cnbc.com](http://www.cnbc.com)



## **ONC's Rucker calls out hospital leaders who signed Epic's opposition letter**

WASHINGTON, D.C.—Federal health IT leader Donald Rucker, M.D., said "Most of their customers did not sign on to that letter," Rucker said. "If you parse out the big academic medical centers, only three out of 100 AMCs signed on."

Source: [www.fiercehealthcare.com](http://www.fiercehealthcare.com)

# HHS Leadership Rejects Scare Tactics to Derail API Rules



“I want to be quite clear: Patients need and deserve control over their records,” **HHS Secretary Alex Azar** said at the *ONC’s annual meeting on January* .

“Unfortunately, ***some are defending the balkanized, outdated status quo*** and fighting our proposals fiercely.” He added: ***“Scare tactics are not going to stop the reforms we need.”***



And **CMS Administrator Seema Verma** *at the Center for Consumer Information and Insurance Oversight’s Industry Day* said on January 29 that ***“disingenuous efforts by certain private actors to use privacy - vital as it is - as a pretext for holding patient data hostage is an embarrassment to the industry.”***

# With a “Privacy by Design” Architecture, Patient-Facing Apps like iBlueButton Offer Unmatched Privacy & Security Protection



## HUMETRIX STATEMENT OF iBLUEBUTTON APP PRIVACY PRACTICES

The following is Humetrix's full statement of privacy practices for its iBlueButton app. **A SHORTER PRIVACY NOTICE IS AVAILABLE [HERE](#).**

Humetrix is dedicated to protecting the privacy rights of users of the App. Our policies with respect to the handling of personal information with respect to the App are described within this Privacy Statement.

We may change, add, or remove portions of this Statement of Privacy Practices at any time, and such changes shall become effective immediately upon posting. **CONTINUED USE OF THE APP FOLLOWING THE POSTING OF CHANGES TO THE PRIVACY POLICY WILL MEAN THAT THE USER ACCEPTS SUCH CHANGES.**

### Information We Collect, Why We Collect It and Who Sees It.

Humetrix automatically collects technical data and related information about the user's device, operating system and application software that is gathered to facilitate the provision of application updates, identify problems with the application, and provide product support to the user of the App. This information does not identify the user.

Humetrix automatically collects information that does not personally identify you about the use of the App, such as information indicating that the App has been used to retrieve a patient record. The App is not supported via advertising and does not use the data it collects for advertising purposes.

### Information We Do Not Collect

Patients who use the App control the entry or receipt of individually identifiable health information when using the App. This information includes demographic information (name, address and date of birth), information about the patient's past, present or future physical or mental health conditions, health care services the patient has received, past, present or future payment for healthcare. Humetrix does not collect this information. This information resides on the user's smartphone or tablet and is not accessible by Humetrix.

The App allow users to take photos from within the App. Humetrix does not collect or have access to any information that the user stores through the App's functionalities.

The App does not collect personally identifiable information about a user's online activities over time and across third-party Web sites or online services. The App does not collect precise information about the location of a user's mobile device.

Users may choose to backup encrypted information to the iCloud server (for iPhone App users) or to Google Drive (for Android App users). No backup information is accessible by Humetrix.

The Humetrix logo, featuring the word "huMETRIX" in a sans-serif font with a red underline under the "hu" portion.

## OUR PRIVACY NOTICE


Below is information about how we handle your personal data.

Touch icons for additional information

### USE

How we use your data internally

We DO NOT collect and use your identifiable data




### SHARE

How we share your data externally with other companies or entities

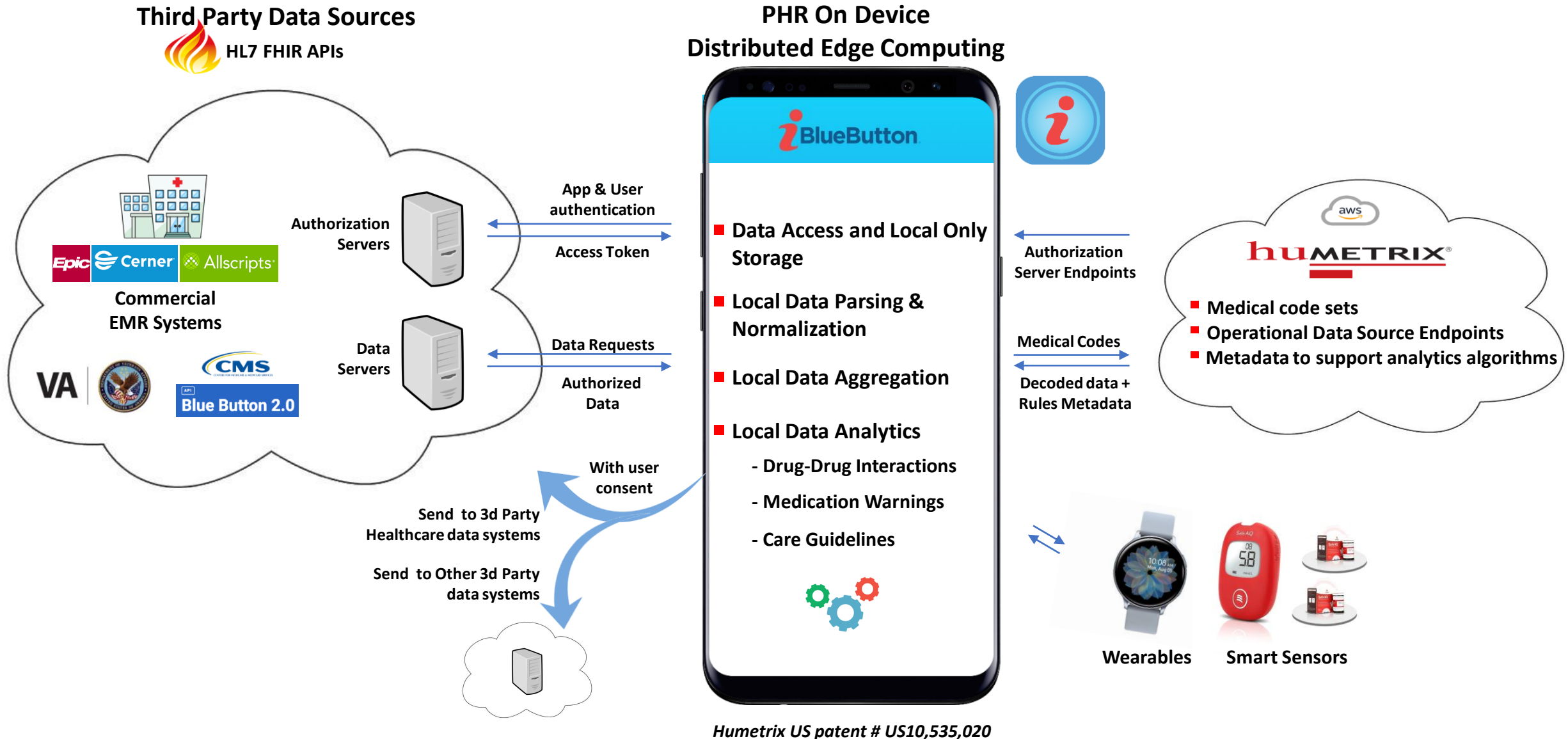
We DO NOT share your identifiable data



We DO NOT share your data AFTER removing identifiers  
(note that remaining data may not be anonymous)



# iBlueButton "Privacy by Design" Architecture







# It's Not the Wild West!

## Government and Industry Have Privacy & Security Protections in Place

Consumer Technology Association CES

TOPICS WHO WE ARE RESOURCES GET INVOLVED JOIN CTA

Press Release | September 12, 2019

### CTA Releases Industry-Developed Privacy Guidelines on Health Data

by Danielle Cassagnol, 703-907-5253, dcassagnol@CTA.tech

carin Enabling consumers and their authorized caregivers to access more of their digital health information with less friction.

HOME WHO WE HELP OUR WORK OUR MEMBERSHIP EVENTS ABOUT US

## Trust Framework and Code of Conduct

### THE CARIN ALLIANCE CODE OF CONDUCT

**Background:** The CARIN Alliance Code of Conduct represents the consensus view of a group of multi-sector stakeholders that include leading providers, payers, health IT companies, EHR companies, consumer platform companies, consumers, caregivers and others focused on advancing consumer-directed exchange across the U.S. The Code is based on internationally recognized standards including the Code of Fair Information Practices (CFIP) (indicated in *italics* below) and numerous other consumer information sharing accepted principles and practices. The Alliance is working collaboratively with other stakeholders and leaders in government to overcome the policy, cultural, and technological barriers to advancing consumer-directed exchange.



VA



U.S. Department of Veterans Affairs



State of California Department of Justice

XAVIER BECERRA  
*Attorney General*

HOME ABOUT MEDIA CAREERS REGULATIONS RESOURCES PROGRAMS CONTACT

## California Consumer Privacy Act (CCPA)

Home / Privacy / California Consumer Privacy Act (CCPA)

### Background on the CCPA & the Rulemaking Process

The California Consumer Privacy Act (CCPA), enacted in 2018, creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. It also requires the Attorney General to solicit broad public participation and adopt regulations to further the

# Why 61M Medicare Beneficiaries & Their Caregivers Need Access via APIs? *To Prevent Diagnostic Errors, Redundancies and Waste*

In a given year, the average Medicare patient visits...



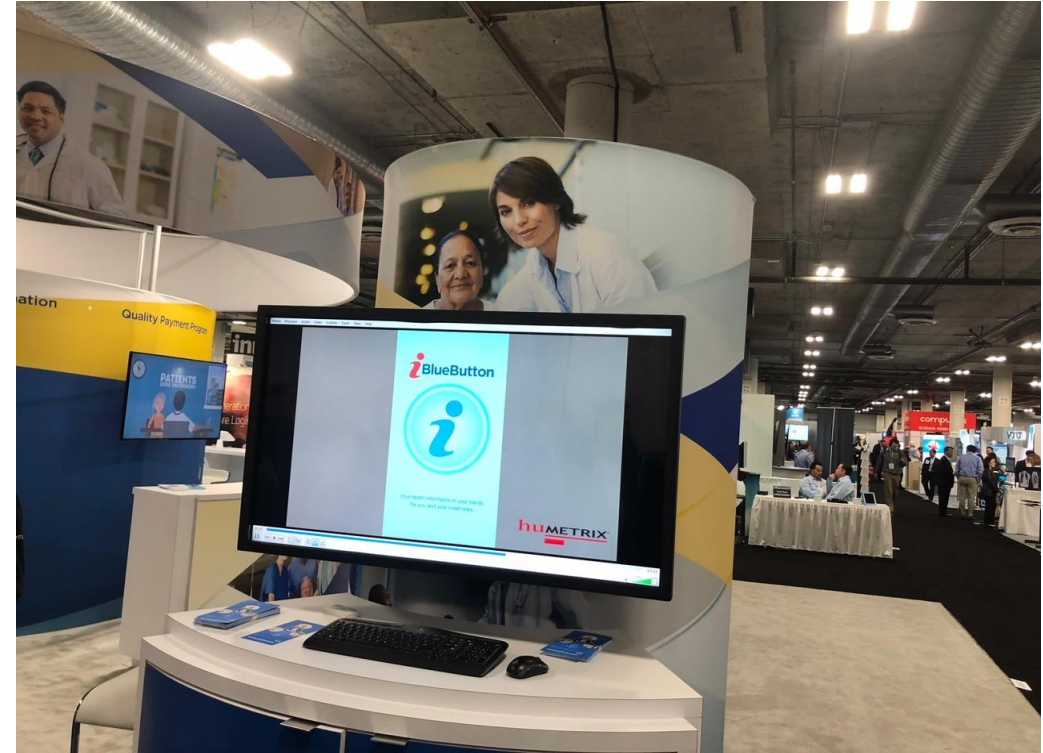
**400,000 Americans die every year of preventable medical errors**

20% of these deaths are caused by a lack of the patient history at the point of care

**1/3 healthcare expenses are wasted in medical errors or redundant care**



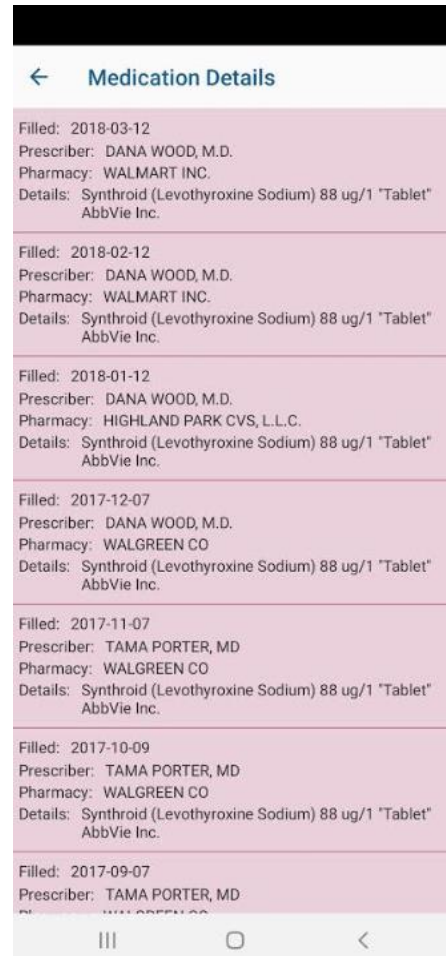
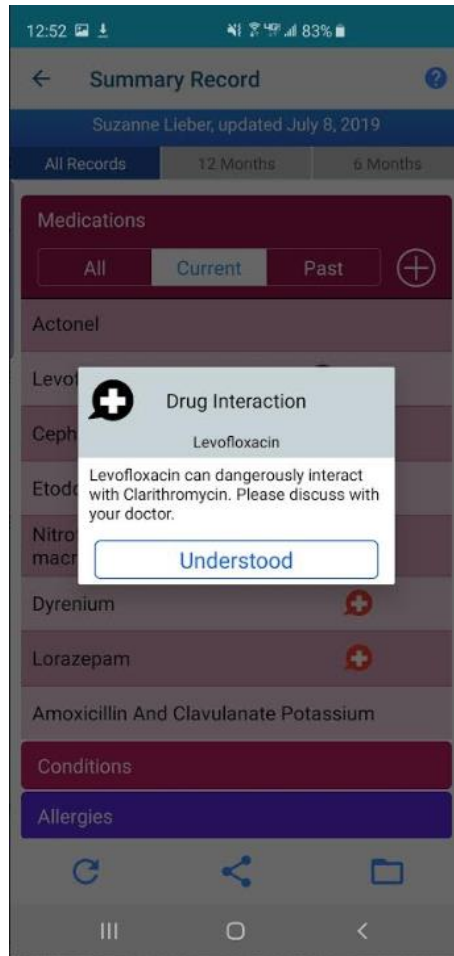
# CMS Blue Button 2.0 API - launched in 2018 for All Medicare FFS Beneficiaries to Access their Medical Data: the API Model for ONC & CMS Rules



**Diagnoses + Medications + Providers + Preventive Services**  
**Outpatient encounters + Hospitalizations + ED Visits**  
**Surgical Procedures + Laboratory & Radiology + Financial Data**



# How API-Enabled Patient Facing Apps Can Be Life-Saving: The Common and Prevalent ADE Example



**37% of Medicare Prescriptions produce  
an iBlueButton Drug Warning**





# APIs - Do Matter

Enabling HIPAA Right of Access

+

Key to Interoperability

=

Patient Safety

## National HIPAA Summit

March 4, 2020

Bettina Experton, M.D., M.P.H.

@BettinaExperton