U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Key Considerations: HIPAA Security, Health IT, and the App Ecosystem

Linda Sanches

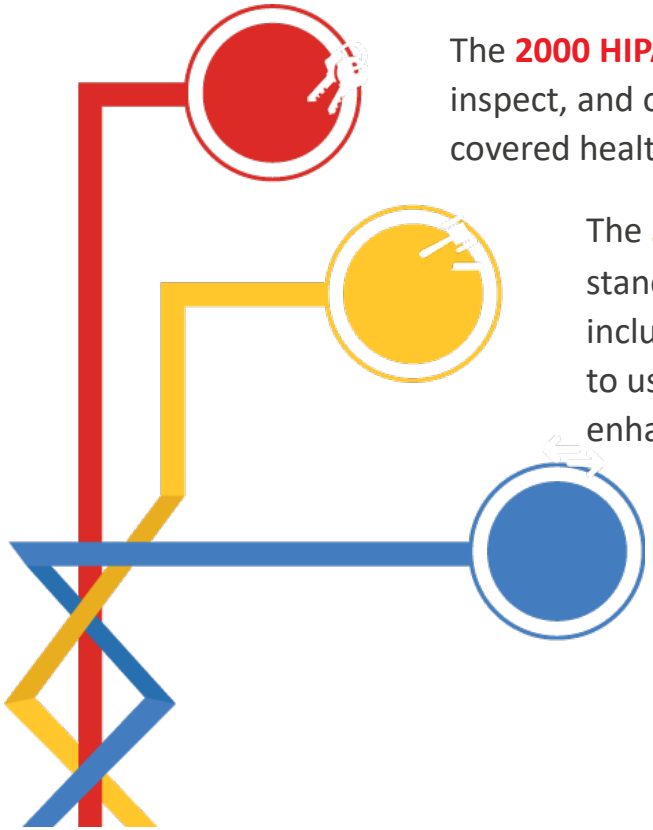
October 2019

Individual Access & Business Associates & Apps

Access, HIPAA & Electronic Health Information (eHI) Exchange

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Recent laws work with existing HIPAA rights to simplify how health care providers can meet individual requests for access to electronic health information



The **2000 HIPAA Privacy Rule** established an individual's right to access, inspect, and obtain a copy of health records, upon request, from a covered health care provider or health plan

The **2009 HITECH Act** directs HHS to adopt certification standards for electronic health record systems (EHRs), including methods for access, and to create rules for providers to use EHRs to provide individual access under Medicare enhanced payment programs

The **2016 Cures Act**

TEFCA: eHI exchange through health information networks (HINs)

Requires certified HIT to publish APIs

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Background: *HIPAA Access*

An individual has the right to request & receive a copy of medical, payment, and other records—Protected Health Information (PHI)—that providers and health plans use to make decisions about individuals

- Doesn't matter how old the PHI is, where it is kept, or where it originated
- Includes clinical lab test reports and underlying information

An individual has the right to receive the information electronically & in her preferred form and format if the entity has the ability to readily produce it

45 CFR 164.524

www.HHS.gov/HIPAA

HITECH Reinforced Individual Right of Access to ePHI

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

If a covered health care provider or health plan uses an EHR that holds an Individual's PHI:

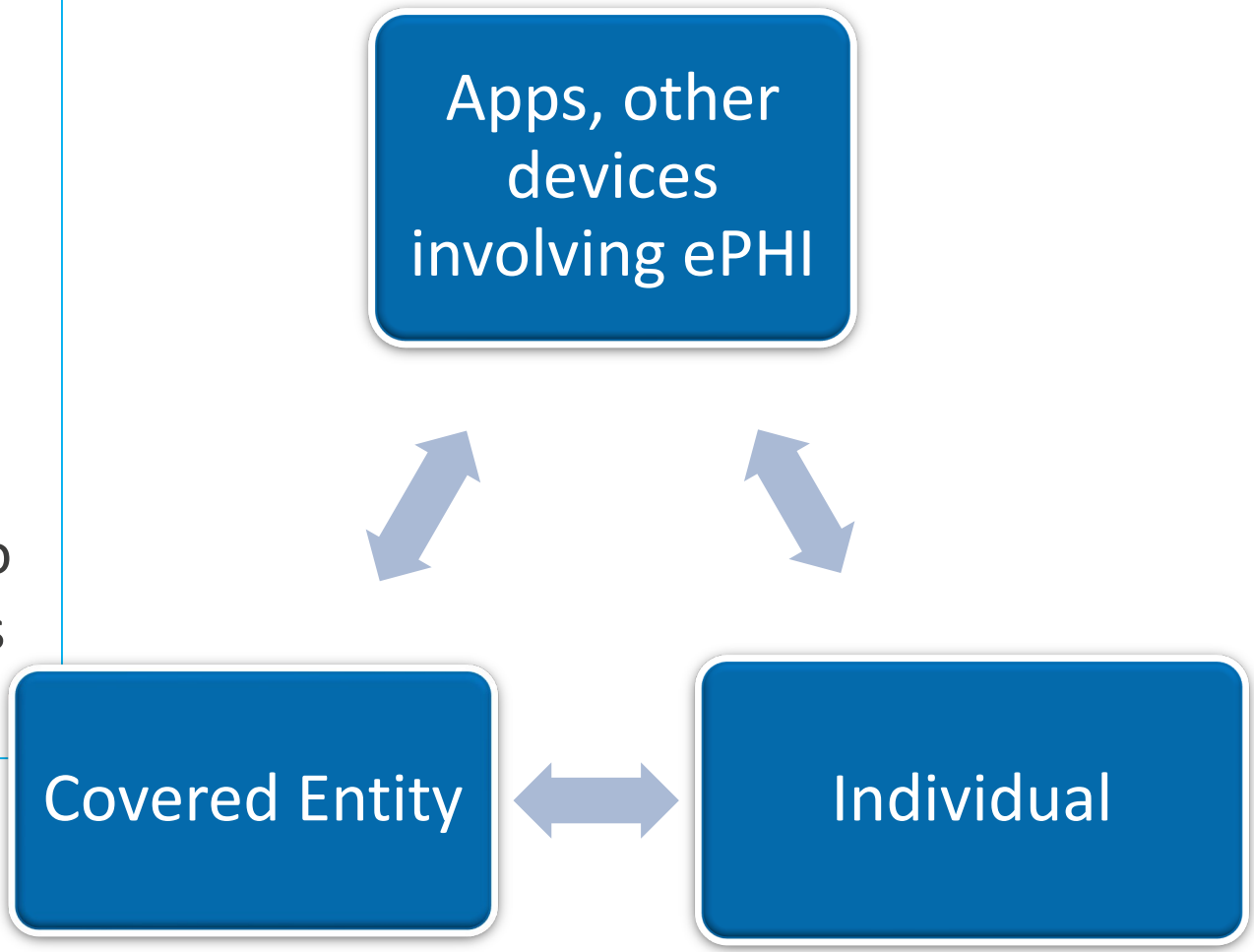
- The individual has a right to obtain a copy of that PHI in an electronic format and
- To direct the provider or plan to transmit the copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific

See HITECH 13405(e)

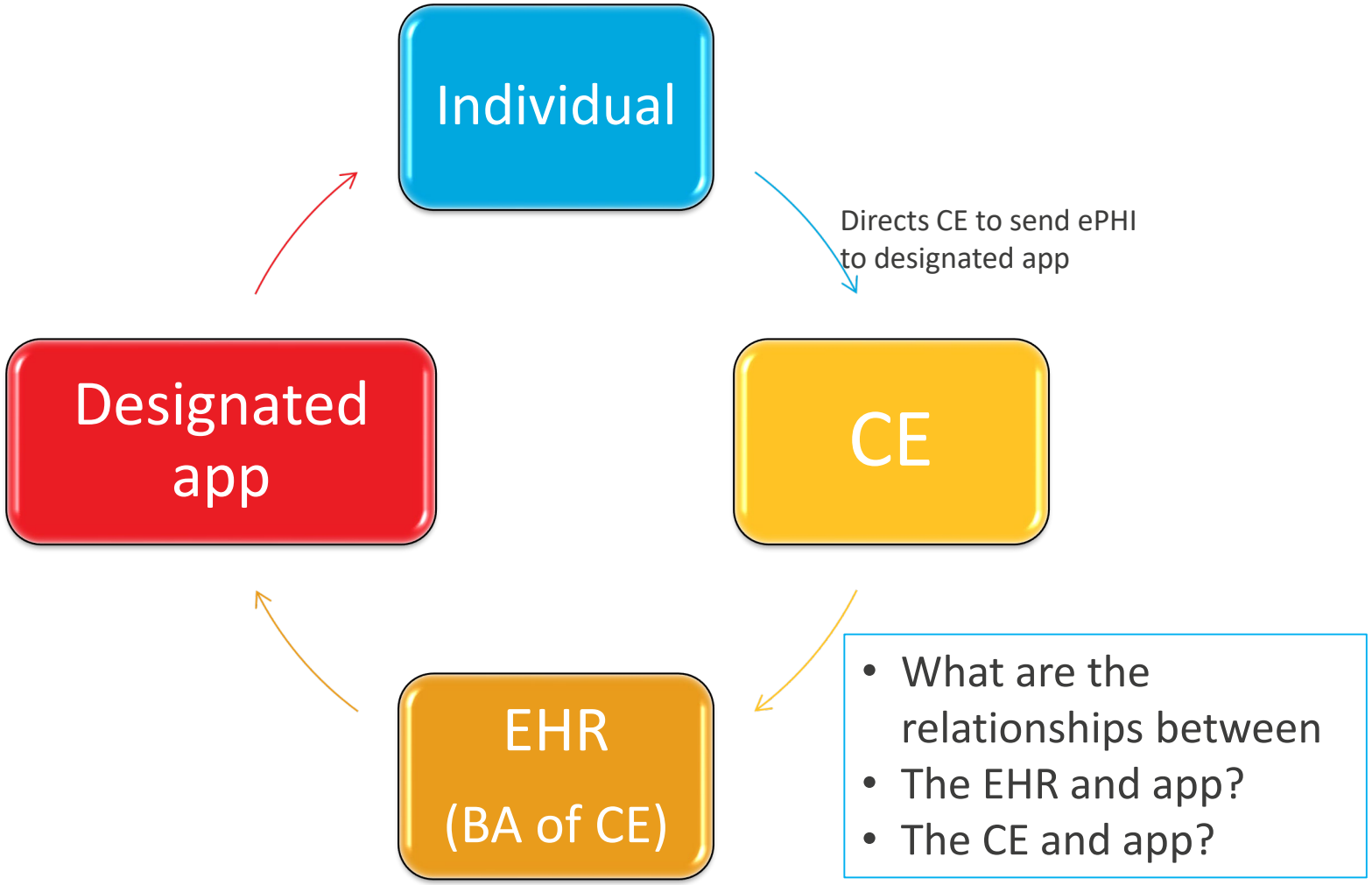
HIPAA Security Requirements & PHI Transmitted Between Entities

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

- What is the relationship between the CE and health IT developer?
- Does the CE contract with app/other tech to provide functions for CE?



CE, EHR and App



HIPAA Access Right, APIs & Health Apps

- 5 FAQs posted on OCR HIPAA website April, 2019
- Supplement the *Health App Use Scenarios* document

https://www.hhs.gov/hipaa/for-professionals/faq/health-information-technology/index.html

FAQ 3010 Covered Entity Liability for Unsecure Transmission

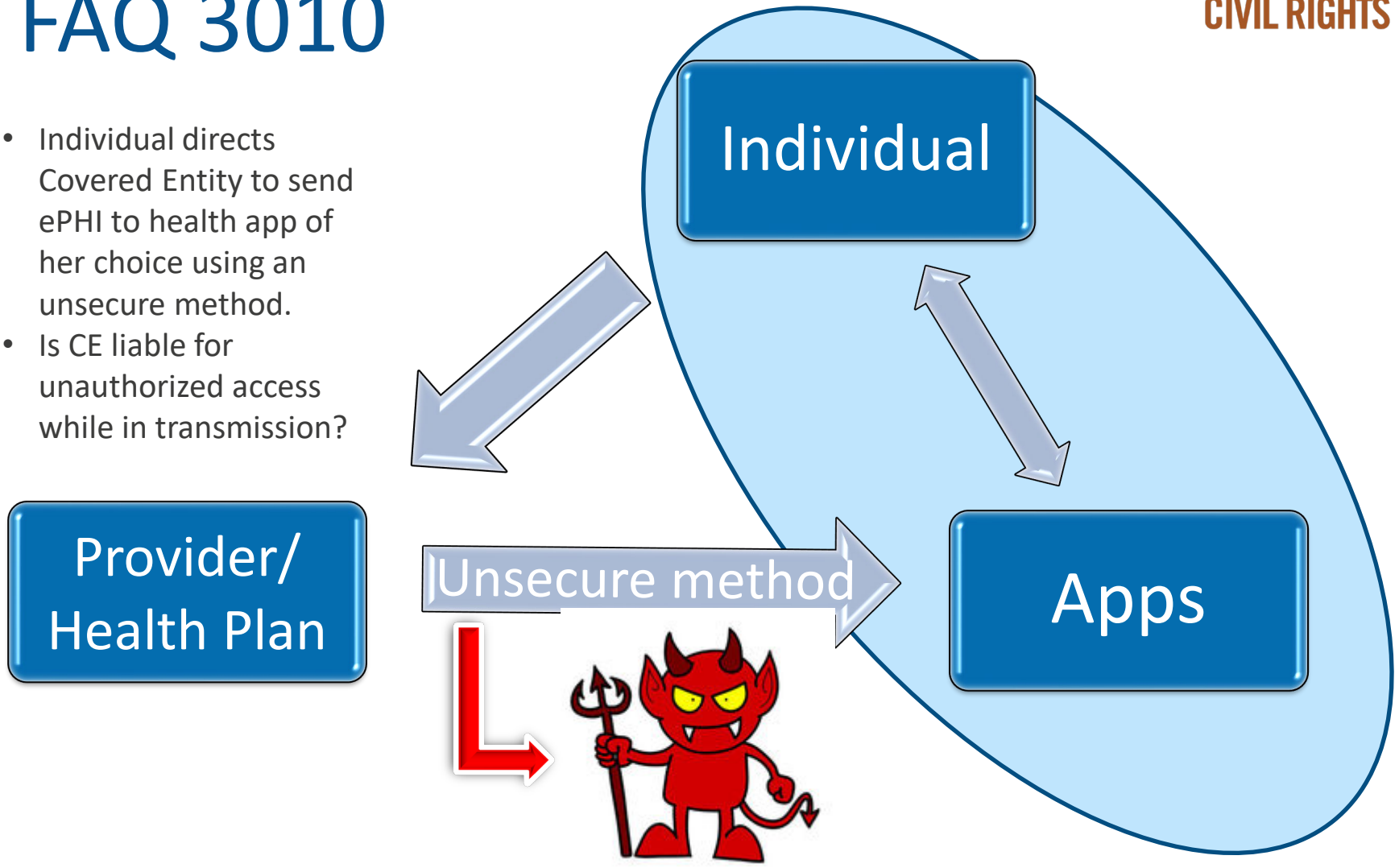
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

- What liability does a covered entity face if it fulfills an individual's request to send their ePHI using an unsecure method to an app?

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

FAQ 3010

- Individual directs Covered Entity to send ePHI to health app of her choice using an unsecure method.
- Is CE liable for unauthorized access while in transmission?



The Upshot: Health Apps, Individual Access & Business Associates

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

If requested by an individual, a health care provider or health plan must transmit an individual's PHI directly to another person or entity designated by the individual—e.g., a health app

App developer acting only on behalf of the individual *is not* subject to HIPAA Rules regarding the health information it creates, maintains, receives from or transmits to a covered entity

App developer creating, receiving, maintaining or transmitting protected health information (PHI) *on behalf of a covered entity* or another business associate is itself a business associate

App developer that is a business associate *is subject* to HIPAA Rules, and must have a business associate agreement with covered entity (or business associate)

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Mobile Health Apps Interactive Tool

Produced in cooperation with the U.S. Department of Health & Human Services (HHS): the Office of the National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA)

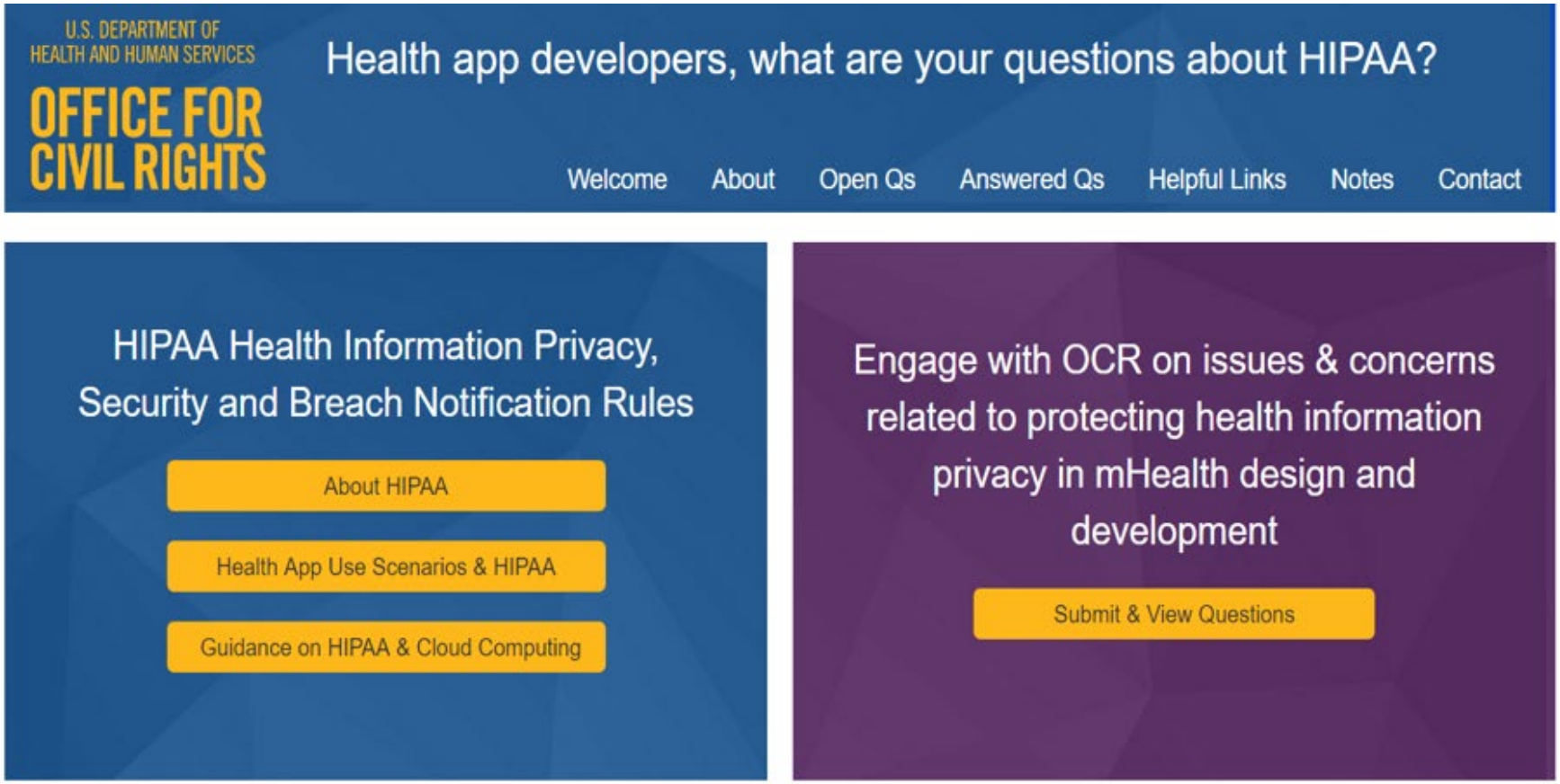
The Office of the National Coordinator for Health Information Technology

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

FDA

OCR Developer Portal

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

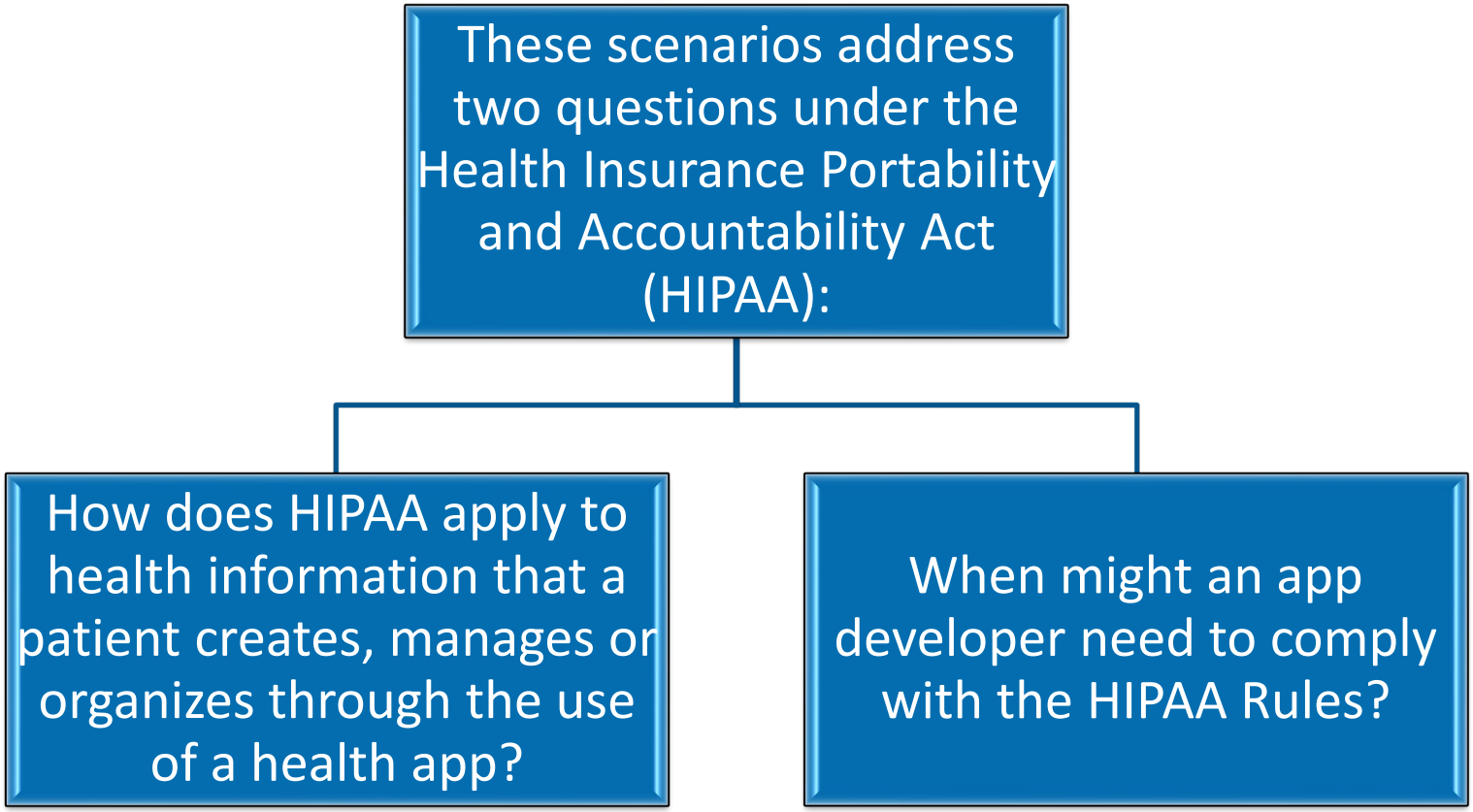


http://hipaaQsportal.hhs.gov/

About

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Health App Use Scenarios & HIPAA



http://hipaaQsportal.hhs.gov/

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Questions?

- Visit us at http://www.hhs.gov/HIPAA
- Follow us on Twitter @HHSOCR
- Join our Privacy and Security listservs at https://www.hhs.gov/hipaa/for-professionals/list-serve/