Health Data Privacy Considerations in the App Economy

HL7 FHIR DevDays – Virtual 2020

Kathryn Marchesini, JD, CISSP
Chief Privacy Officer

The Office of the National Coordinator for Health Information Technology

Please Note:

- The materials contained in this presentation are based on the provisions contained in the relevant statutes and regulations. While every effort has been made to ensure the accuracy of the restatement of those provisions, this presentation is not a legal document. The official program requirements are contained in the relevant laws and regulations. Please note that other Federal, state, and local laws may also apply.

- This communication is produced and disseminated at U.S. taxpayer expense.

Today's Topics

- Snapshot of federal regulatory structure of mHealth
- Overview of key U.S. federal privacy and security laws and regulations in digital health
- Determining which federal law/regulation(s) may apply
- Situational awareness & other considerations
- Summary tips

The Office of the National Coordinator for Health Information Technology

Snapshot of Federal Oversight of Privacy & Security of Health Information + Mobile Health App Developers

Federal Role in mHealth

If you are developing an app for or provided by or on behalf of a health care provider or plan, then…	*If your app collects information directly from consumers or specifically targets children, then…*	*If your app gets certified or a health care provider uses it as part of a certified health IT product, then…*	*If your app is a medical device, then…*	*If you are a telecommunications carrier or interconnected VoIP provider, then…*
HIPAA Rules	**FTC Act, Health Breach Notification Rule, & COPPA Rule**	**ONC Cures Act Final Rule**	**FD&C Act**	**Telecommunications Act & CPNI Rules**

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

The Office of the National Coordinator for Health Information Technology

FDA

FCC

The Office of the National Coordinator for Health Information Technology

HIPAA Rules – 5,000 Foot View

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

Privacy Rule
Which health information must be protected, responsibilities of covered organizations, and what individual rights exist

Security Rule
How to safeguard health information (administrative, physically, and technical)

Breach Notification Rule
Who to notify in a breach situation

Enforcement Rule
Who enforces HIPAA and what penalties exist

More information available on HHS OCR's website: https://www.hhs.gov/hipaa/index.html

HIPAA – Data Privacy and Security: The Whos & Whats

WHO must comply? *"Covered Entities & Business Associates"*	• Health care providers (e.g., physicians, nurses, clinics, hospitals, pharmacists) • Health plans (e.g., health insurers) • Clearinghouses • Persons or entity who performs certain functions or activities *on behalf of* a covered entity that involve the use or disclosure of PHI ("business associates")

WHAT data must be protected?
"Protected Health Information"
	• "Protected health information" – broadly defined individually identifiable health information created or received by an entity covered by HIPAA
	• *"Information…that relates to the individual's past, present, or future physical or mental health…the provision of health care to the individual, or payment for the provision of health care to the individual"*
	• De-identified information is NOT protected
	  • Safe harbor (remove 18 listed identifiers)
	  • Statistical method

WHAT data protection obligations do entities have? *"Privacy & Security Requirements"*	• Conditions for using and disclosing (sharing) PHI ("treatment, payment, or health care operations"; minimum necessary; when individual authorization required • Individual/patient rights, including access to health information • Technical, administrative, and physical safeguards and breach notification

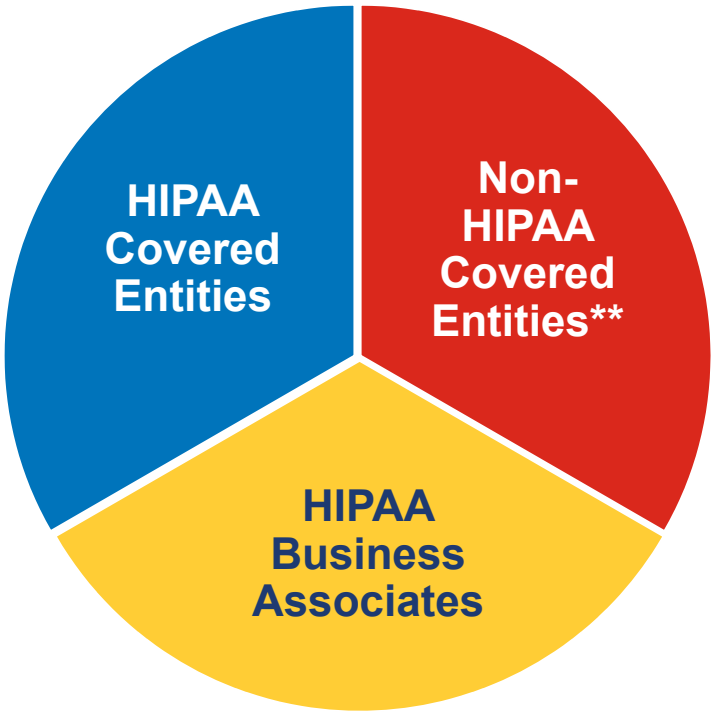
An App Developer May Be A *Business Associate* under HIPAA

If the developer is creating or offering the app on behalf of a covered entity (or one of the covered entity's contractors)…

In general, a business associate is a person [or entity] who creates, receives, maintains or transmits protected health information (PHI) on behalf of a covered entity or another business associate.

In that case, the developer is required to comply with certain provisions of the HIPAA Rules, including entering into a business associate agreement (BAA) with the covered entity.

General Categories of Federally-Regulated Actors* (for Electronic Health Information Privacy Purposes)



*Generally, Section 5 of the FTC Act applies (to for-profit organizations), which does not depend on whether the organization/conduct is regulated/covered by the HIPAA Rules.
**The FTC's Health Breach Notification Rule applies to certain types of entities that fall outside of the scope of HIPAA, and therefore, are not subject to the HIPAA Breach Notification Rule.

Some ONC Activities Relevant to Non-HIPAA Covered Entities

Report to Congress on Information Blocking

https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

Report to Congress on Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA

https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

Model Privacy Notice

https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn

Guide to Getting & Using Your Health Records

https://www.healthit.gov/how-to-get-your-health-record/

FTC Act Fundamentals

Section 5 of the FTC Act broadly prohibits "unfair or deceptive acts or practices in or affecting commerce."

- **Unfairness**: a practice that causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers
- **Deception**: a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances

Section 5 authority extends to both HIPAA and non-HIPAA covered entities

Learn more about the FTC's authority: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

Health Breach Notification Rule*

**Does not apply to entities covered by HIPAA*

Applies to three types of entities:

- Vendors of personal health records (PHRs)
- PHR-related entities
- Third-party service providers

Requires these entities that suffer a breach to notify:

- Everyone whose information was breached
- The FTC
- In some situations, notify the media

FTC' s Public Comment Period on this Rule Closes August 20, 2020

Children's Online Privacy Protection Act (COPPA) Rule

- **Applies to the operator of any commercial website or online service (including a mobile app) that**
  - Is directed to children under 13 or
  - Where the operator has actual knowledge that it collects, uses, or discloses personal information from children under 13
- **Requires operators to**
  - Give parents notice of what personal information the operator is collecting from children
  - Get parent's verifiable consent (before collecting children's personal information)
  - Institute reasonable security for information collected from children online

Review FTC's COPPA FAQs: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

The Office of the National Coordinator for Health Information Technology

ONC Cures Act Final Rule: Third-Party App Developer "Pathways"

Third-Party App Developer – Two General Paths:

ONC's Cures Act Final Rule

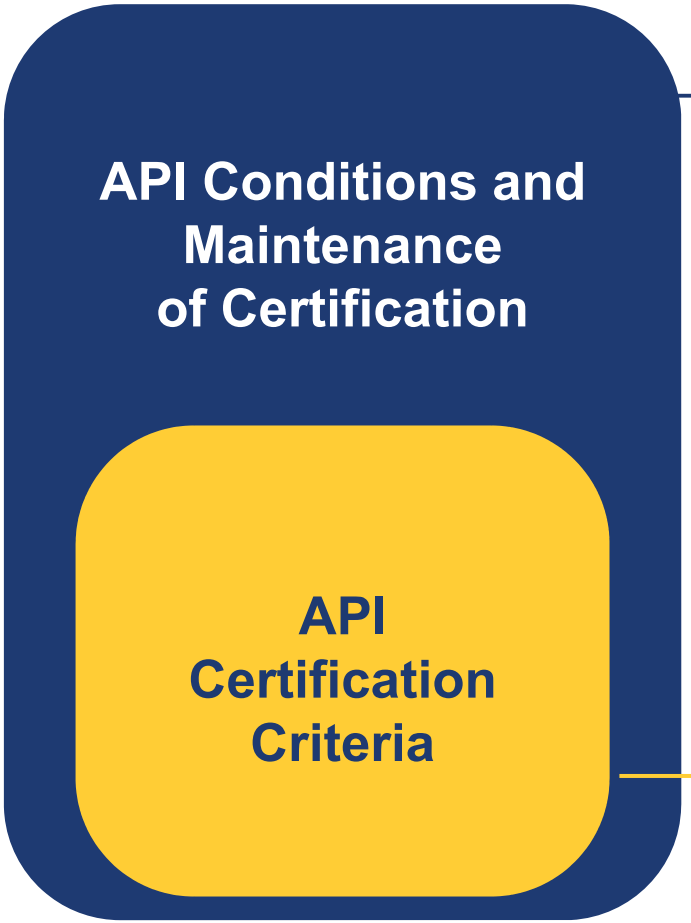
"Actor" (e.g., Certified API Developer)

If developing **an app** on behalf of a health care provider, or thinking about getting an app certified under the ONC Health IT Certification Program, then review the Rule's **certification requirements** for **Certified API Developers**.

API User

If developing **a third-party app** that is patient-directed that will interact with "certified API technology," then as an **API User**, review the following Rule highlights...

Application Programming Interfaces – § 170.404



API Conditions and Maintenance of Certification

Applies to actions and behaviors of certified health IT developers related to the use of their Certified API Technology

API Certification Criteria

- Certified API criteria (§ 170.315(g)(7) through (10))
- Scope of EHI limited to United States Core Data for Interoperability (USCDI)
- Includes new 2015 Edition Secure, Standards-Based API criteria (§ 170.315(g)(10))
  - “read-only” focus
  - HL7® FHIR® Release 4.0.1 as base standard
  - Support for single patient and population services

Snapshot of API Condition & Maintenance of Certification Requirements – Indirect Impacts on API Users

- **API Conditions of Certification Requirements**
  - Provide new transparency requirements on certified API developers
  - Set criteria for allowable fees
  - Set business requirements that certified API developers will have to comply with for their certified API technology to promote an open and competitive marketplace

- **API Maintenance of Certification Requirements**
  - Address ongoing requirements that must be met by certified API developers and their certified API technology
  - Establish requirements for certified API developers related to use of certified API technology adopted in § 170.315(g)(10)
    - Authenticity Verification
    - Application Registration
    - Service Base URL Publication

Information Blocking

What is information blocking?

A practice by a health care provider, health IT developer, health information exchange, or health information network that, except as required by law or specified by the **Secretary as a reasonable and necessary activity**, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

What are the exceptions?

- Section 4004 of the Cures Act authorizes the Secretary to identify reasonable and necessary activities that do not constitute information blocking.
- The Rule identifies eight exceptions for practices that are reasonable and necessary, provided certain conditions are met.

INFORMATION BLOCKING

Three categories of "Actors":

- Health Care Providers
- Health IT Developers of Certified Health IT
- Health Information Exchanges and/or Health Information Networks

"Interfere with" or "Interference"

Interfere with or interference means to prevent, materially discourage, or otherwise inhibit.

Examples of Interferences

- Withholding "FHIR service base URLs" (also referred to as "FHIR endpoints")
- Delays in access, exchange, or use
- Fees for electronic access by patients/individuals
- "Vetting" third-party apps
- Requiring third-party apps, chosen by patients/individuals, to sign a contract/BAA for electronic access

"Interfere with" or "Interference" – What is it not?

- ***Educating patients about privacy & security risks of their chosen third-party apps*** – Actors may provide patients with information that:
  - Focuses on any current privacy and/or security risks posed by the technology or the third-party developer of the technology;
  - Is factually accurate, unbiased, objective, and not unfair or deceptive; and
  - Is provided in a non-discriminatory manner.
- ***Following existing BAAs or service level agreements*** – Actors are **not** required to violate BAAs or associated service level agreements.
  - However, a BAA or its associated service level agreements must not be used in a discriminatory manner by an actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule.

Federal Food, Drug, and Cosmetic Act (FD&C Act)

- Regulates the safety and effectiveness of medical devices, including certain "mobile medical apps"
- Focuses on a small subset of health apps that pose a higher risk if they don't work as intended
- Requires FDA approval in certain circumstances
  - Examples of device software functions (including mobile medical applications) that are considered medical devices that the FDA regulates
  - Examples of mobile apps that are not medical devices available on FDA's website

FDA's Policy for Device Software Functions and Mobile Medical Applications Guidance provides more details.

Telecommunications Act & CPNI Rules

Seeks to protect Customer Proprietary Network Information (CPNI)

- **Applies to**
  - Telecommunications carriers
  - VOIP Providers
- **Requires carriers to**
  - Follow certain use and disclosure rules
  - Implement certain safeguards
  - Notify law enforcement and affected customers, if breach of certain information

Learn more about the FCC's CPNI Rules: https://www.fcc.gov/general/customer-privacy

mHealth Apps Interactive Tool

Tool Accessible Here:

https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

Where to Start? Which Federal Laws May Apply? Is an App Developer Subject to HIPAA?

START

Does your health app create, receive, maintain, or transmit identifiable (health) information?

Who are your clients?
How are you funded?
Are you or your clients covered entities?

e.g., hospitals, doctor's offices, clinics, pharmacies, health insurance issuers; health or wellness program related to a health plan offered by an employer

Were you hired by, or are you paid for your service or product by, a covered entity? Or another business contracted to a covered entity?

Does a covered entity (or a business associate acting on its behalf) direct you to create, receive, maintain or disclose information related to a patient or health plan member?

From *Health App Use Scenarios and HIPAA*, available on the OCR Developer Portal

FTC Act & Health Breach Notification Rule – Do they Apply?

Does your mobile app collect, create, or share consumer information?

Are you a nonprofit organization?

Do you offer health records directly to consumers (or do you interact with or offer services to someone who does)?

Are you developing this app as or on behalf of a HIPAA covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program)?

COPPA Rule – Does it Apply?

Is your app intended for children?

Does your app use child-oriented activities, incentives, design, music, or the like?

Do you have actual knowledge that children are using your app?

ONC Cures Act Final Rule – Does it Apply?

Are you a health care provider, health information network or health information exchange, or a health IT developer of certified health IT, as those terms are defined in the ONC Cures Act Final Rule?

Is your app designed to access, exchange, or use electronic health information at the direction of/on behalf of a consumer/patient, but an "actor" (or the actor's app) for information blocking purposes?

Does your app access, exchange, or use patient information from a HIPAA covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program) at the direction of a patient, including through a secure, standards-based API?

Is your app, or any other app/health IT you have developed, part of/a health IT product certified under the ONC Health IT Certification Program?

FDA Act – Does it Apply?

Is your app intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease?

Does your app pose "minimal risk" to a user?

Is your app a "mobile medical app?"

U.S. Federal Role in mHealth

Key U.S. Federal Laws & Regulations that Apply to Health Information

Which federal laws may apply to me and my health app?

HIPAA Privacy, Security, & Breach Notification Rules

- ✓ Does your app create, receive, maintain, or transmit identifiable information?
- ✓ Is the health information your app will/plans to access, collect, exchange, share, use, or maintain identifiable health information?
- ✓ Are your clients a health care provider or health plan?
- ✓ Are you developing this app on behalf of a HIPAA covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program)? Or are you acting as subcontractor to another entity providing services to a covered entity?

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

FTC Act & Health Breach Notification Rule

- ✓ Does your mobile app collect, create, or share consumer information?
- ✓ Are you a nonprofit organization?
- ✓ Are you developing this app as or on behalf of a HIPAA covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program)?
- ✓ Do you offer health records directly to consumers (or do you interact with or offer services to someone who does)?

COPPA Rule

- ✓ Is your app intended for children?
- ✓ Does your app use child-oriented activities, incentives, design, music, or the like?
- ✓ Do you have actual knowledge that children are using your app?

FD&C Act

- ✓ Is your app intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease?
- ✓ Does your app pose "minimal risk" to a user?
- ✓ Is your app a "mobile medical app?"

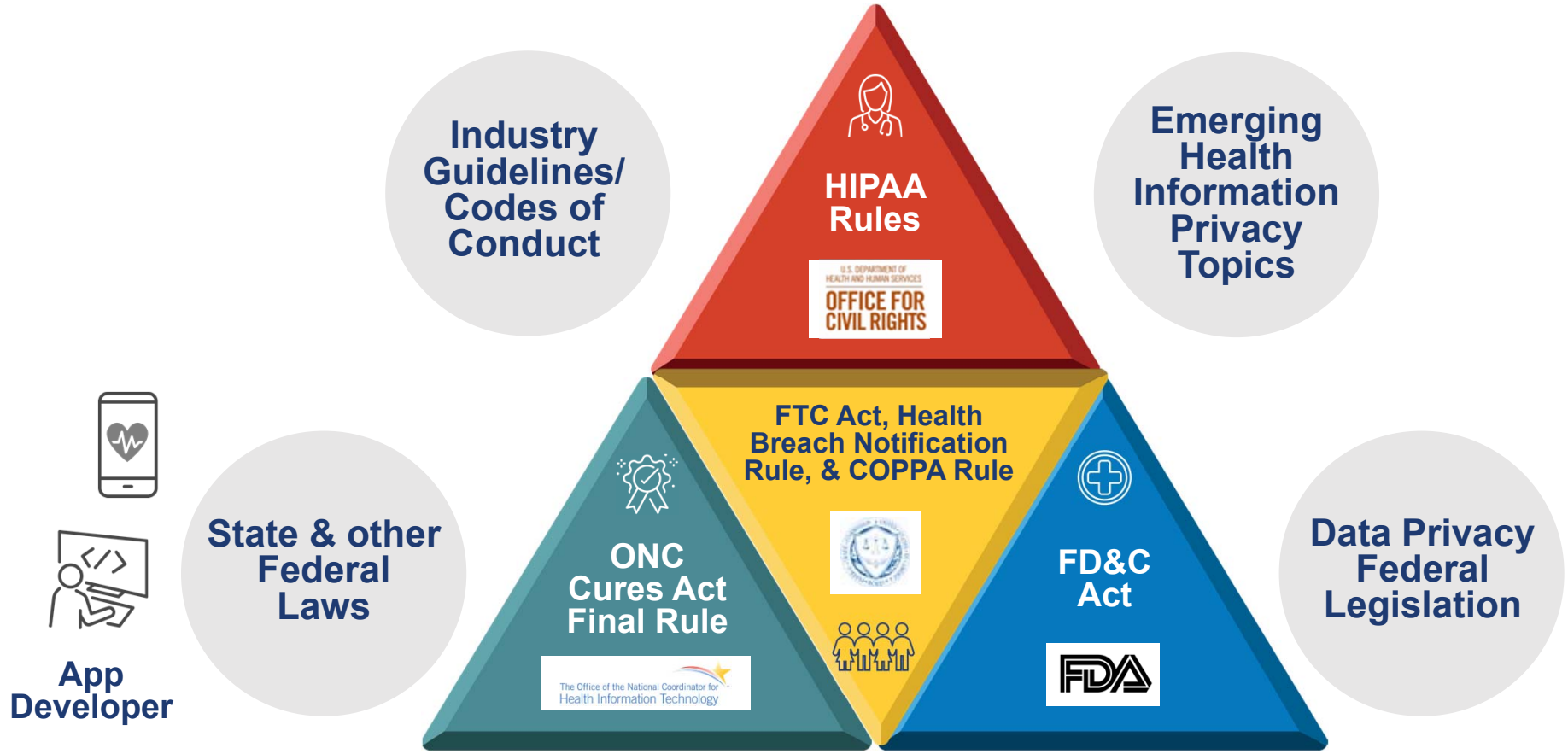
FDA

ONC Cures Act Final Rule

The Office of the National Coordinator for Health Information Technology

- ✓ Are you a health care provider, health information network or health information exchange, or a health IT developer of certified health IT?
- ✓ Is your app designed to access, exchange, or use electronic health information at the direction of/on behalf of a consumer/patient, but an "actor" (or the actor's app) for information blocking purposes?
- ✓ Does your app access, exchange, or use patient information from a HIPAA covered entity at the direction of a patient, including through a secure, standards-based API?
- ✓ Is your app, or any other app/health IT you have developed, part of a health IT product certified under the ONC Health IT Certification Program?

Situational Awareness & Other Considerations Against the Federal Regulatory Backdrop



Summary Tips

- **Determine whether you are a HIPAA covered entity or a business associate**
  - HIPAA applies to health information, only where a covered entity is involved
  - Obligations, rights, and opportunities depend on what you are doing, for whom, and in partnership with whom
- **If HIPAA does not apply, don't stop there – you may need to engage with/be regulated by other federal laws**
  - Answer questions in the Mobile Health Apps Interactive Tool to navigate which law(s) may apply
  - Consider other laws (federal and state) that apply to specific actors and/or types of health information
- **Check out government and industry privacy and security best practices and guidelines** (e.g., ONC's model privacy notice, FTC's Start with Security Guide).

The Office of the National Coordinator for Health Information Technology

Questions?

Kathryn Marchesini
Kathryn.Marchesini@hhs.gov

Twitter: @ONC_HealthIT

LinkedIn: Search “Office of the National Coordinator for Health Information Technology”

HealthIT.gov

Subscribe to our weekly eblast at healthit.gov for the latest updates!