The Office of the National Coordinator for Health Information Technology

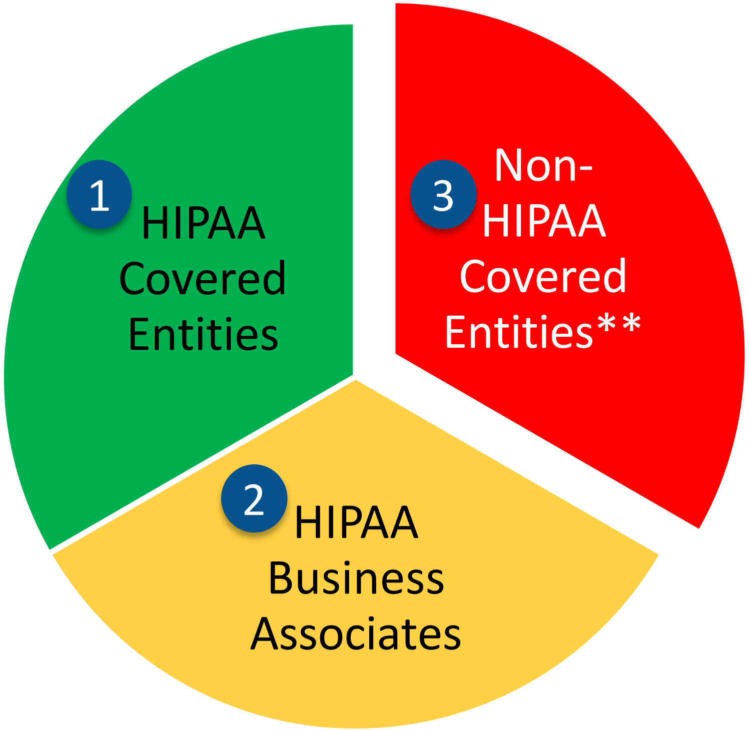
Chief Privacy Officer Update

Kathryn Marchesini, Chief Privacy Officer | HHS/ONC

Today's Topics

- Categories of Regulated Actors
- Individual's HIPAA Right of Access to Health Information
- ONC's Efforts
- Snapshot of Industry Self-Regulatory Approaches
- Resources
- Discussion

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



1 HIPAA Covered Entities

2 HIPAA Business Associates

3 Non-HIPAA Covered Entities**

*Generally, Section 5 of the FTC Act applies (to for-profit organizations) which does not depend on whether the organization/conduct is regulated by/covered by HIPAA.

**The FTC 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.

Individuals' HIPAA Right of Access to Electronic Health Information

Newer laws work with existing HIPAA rights to support 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 plan

The **2009 HITECH Act** directed HHS to adopt certification criteria and standards for electronic health record (EHRs), including methods for access, and establishes an individual's right to a copy of health records in an electronic format (if uses/maintains an EHR), including directing health care providers and plans to transmit a copy directly to the individual's designee (See HITECH 13405(e))

The **2016 Cures Act** directs HHS to adopt conditions of certification to include APIs without special effort and improve patient access to their electronic health information (See Cures Sec. 4006)

Some of ONC's Relevant Activities

3 Non-HIPAA Covered Entities**

Report to Congress on Information Blocking

Cite: 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

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

Model Privacy Notice

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

Guide to Getting & Using Your Health Records

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

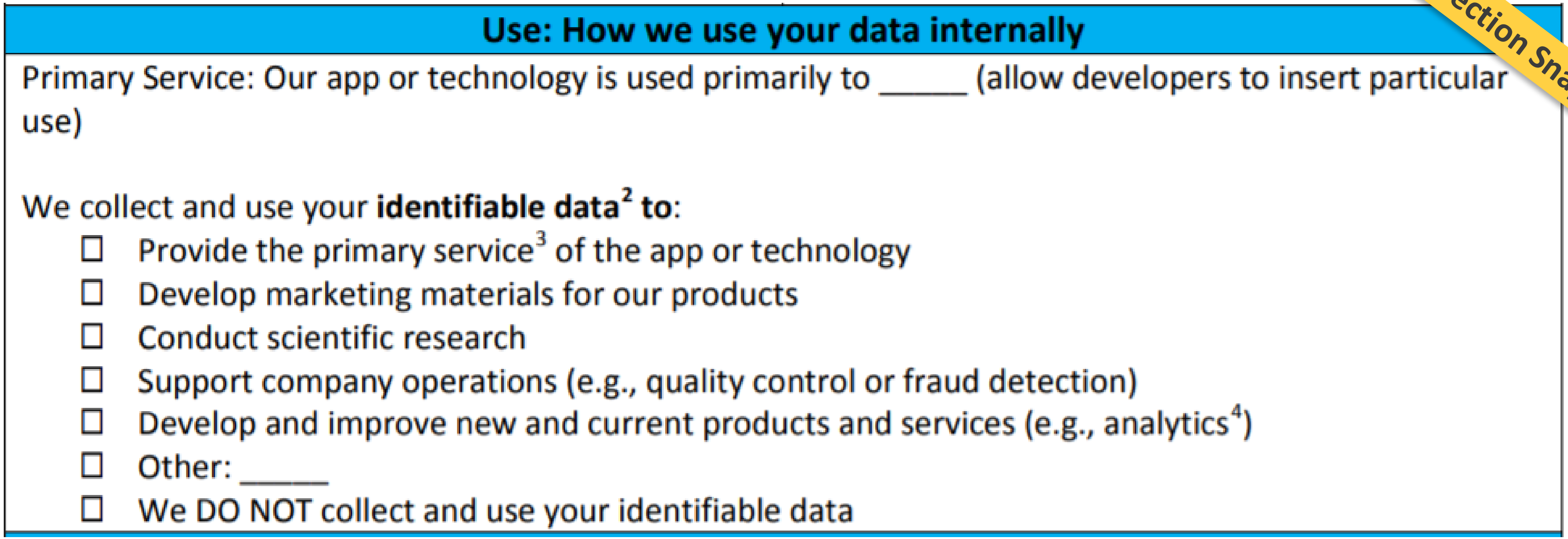
Key Elements of ONC’s Model Privacy Notice (MPN)

- **Use**: How we use your data internally
- **Share**: How we share your data externally with other companies or entities
- **Sell**: Who we sell your data to
- **Store**: How we store your data
- **Privacy**: How this technology accesses other data
- **User Options**: What you can do with the data that we collect
- **Breach**: How we will notify you and protect your data in case of an improper disclosure

MPN continued

3 Non-HIPAA Covered Entities**

MPN Section Snapshot



Use: How we use your data internally

Primary Service: Our app or technology is used primarily to _____ (allow developers to insert particular use)

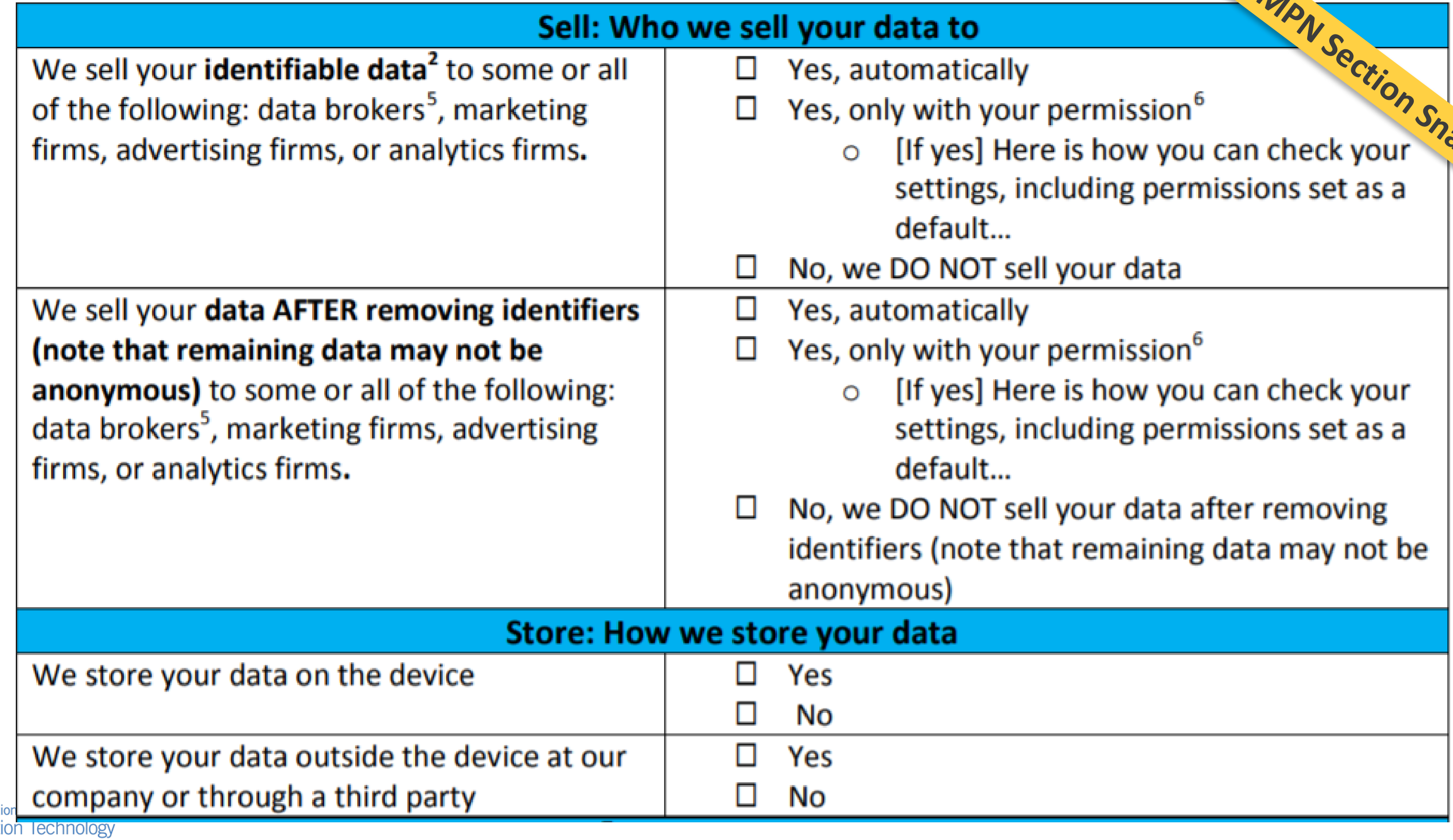
We collect and use your **identifiable data**[2] **to**:

- □ Provide the primary service[3] of the app or technology
- □ Develop marketing materials for our products
- □ Conduct scientific research
- □ Support company operations (e.g., quality control or fraud detection)
- □ Develop and improve new and current products and services (e.g., analytics[4])
- □ Other: _____
- □ We DO NOT collect and use your identifiable data

MPN continued

3 Non-HIPAA Covered Entities**

MPN Section Snapshot



Sell: Who we sell your data to	
We sell your **identifiable data**[2] to some or all of the following: data brokers[5], marketing firms, advertising firms, or analytics firms.	□ Yes, automatically □ Yes, only with your permission[6] ○ [If yes] Here is how you can check your settings, including permissions set as a default… □ No, we DO NOT sell your data
We sell your **data AFTER removing identifiers (note that remaining data may not be anonymous)** to some or all of the following: data brokers[5], marketing firms, advertising firms, or analytics firms.	□ Yes, automatically □ Yes, only with your permission[6] ○ [If yes] Here is how you can check your settings, including permissions set as a default… □ No, we DO NOT sell your data after removing identifiers (note that remaining data may not be anonymous)
Store: How we store your data	
We store your data on the device	□ Yes □ No
We store your data outside the device at our company or through a third party	□ Yes □ No

Health Industry Self-Regulatory Approaches: Codes of Conduct, Principles, & Guidelines

3 Non-HIPAA Covered Entities**

Nationwide Privacy & Security Principles (FIPPs)	CARIN Alliance – Code of Conduct	CTA – Privacy Principles on Health Data	Xcertia™ – mHealth App Privacy Guidelines	ONC Model Privacy Notice
Individual Access	✓	✓		✓
Correction				✓
Openness & Transparency	✓	✓	✓	✓
Choice/Consent	✓		✓	✓
Collection, Use, & Limitation	✓	✓	✓	✓
Safeguards/Security	✓	✓	✓	✓
Data Quality & Integrity	✓		✓	
Accountability	✓	✓		
Other (e.g., selling of data)				✓

NOTIONAL Comparison Example*

*As of September 2019, based on publically available information

Resources

Title/Document	Available URL
ONC – Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information	https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf
The CARIN Alliance – Code of Conduct	http://www.carinalliance.com/wp-content/uploads/2018/11/2018_CARIN_Code_of_Conduct_11262018.pdf
Consumer Technology Association – Guiding Principles for the Privacy of Personal Health and Wellness Information	https://www.cta.tech/cta/media/Membership/PDFs/CTA-Guiding-Principles-for-the-Privacy-of-Personal-Health-and-Wellness-Information.pdf
Xcertia™ – mHealth App Privacy Guidelines	https://xcertia.org/app-privacy-survey/
ONC – Model Privacy Notice	https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf

The Office of the National Coordinator for
Health Information Technology

Discussion & Questions

CONTACT INFORMATION

Kathryn Marchesini
Kathryn.Marchesini@hhs.gov

@ONC_HealthIT

@HHSONC

HealthIT.gov