ONC Policy Overview

Session 66, February 21, 2017

Elise Sweeney Anthony, Director of Policy, ONC
Has no real or apparent conflicts of interest to report.
Learning Objectives

• Describe the relationship between the 2015 Edition certification criteria and Merit-Based Incentive Payment System and Alternative Payment Models providers under the Quality Payment Program.

• Explain ONC’s new rule that enhances surveillance and transparency of health IT.

• Discuss Office of Policy Initiatives
2015 Edition & Supporting QPP through Health IT

Supporting provider & patient needs through certification criteria focused on interoperability
Overview of the 2015 Edition Final Rule

- Builds on the foundation established by the 2011 and 2014 Editions and addresses stakeholder feedback by reducing burden as compared to the 2015 Edition proposed rule
- Focuses on health IT components necessary to advance an interoperable nationwide health information infrastructure
- Incorporates changes designed to foster innovation, open new market opportunities, and provide more provider and patient choices in electronic health information access and exchange
- Addresses information blocking and the continued reliability of certified health IT
2015 Edition Final Rule - Health IT Goals

- Improve Interoperability
- Facilitate Data Access and Exchange
- Ensure Privacy and Security Capabilities
- Improve Patient Safety
- Reduce Health Disparities
- Improve the Reliability and Transparency of Certified Health IT
- Use the ONC Health IT Certification Program to Support the Care Continuum
- Support QPP & the EHR Incentive Programs
2015 Edition: Things to Know

- New Privacy & Security Framework
- Supportive of the broader care continuum
- New and updated vocabulary, content, and transport standards for the structured recording and exchange of health information
  - 2015 Edition Base EHR Definition
  - Common Clinical Data Set
  - Other uses are supported, for example:
    - Public Health
    - Social, Psychological, and Behavioral Health
    - Patient Capture of Health Information
## BASE EHR CAPABILITIES

<table>
<thead>
<tr>
<th>BASE EHR CAPABILITIES</th>
<th>CERTIFICATION CRITERIA</th>
</tr>
</thead>
</table>
| Includes patient demographic and clinical health information, such as medical history and problem lists | Demographics § 170.315(a)(5)  
Problem List § 170.315(a)(6)  
Medication List § 170.315(a)(7)  
Medication Allergy List § 170.315(a)(8)  
Smoking Status § 170.315(a)(11)  
Implantable Device List § 170.315(a)(14) |
| Capacity to provide clinical decision support                                          | Clinical Decision Support § 170.315(a)(9)                                                                                                              |
| Capacity to support physician order entry                                             | Computerized Provider Order Entry (medications, laboratory, or diagnostic imaging) § 170.315(a)(1), (2) or (3)                                      |
| Capacity to capture and query information relevant to health care quality             | Clinical Quality Measures – Record and Export § 170.315(c)(1)                                                                                          |
| Capacity to exchange electronic health information with, and integrate such information from other sources | Transitions of Care § 170.315(b)(1)  
Data Export § 170.315(b)(6)  
Application Access – Patient Selection § 170.315(g)(7)  
Application Access – Data Category Request § 170.315(g)(8)  
Application Access – All Data Request § 170.315(g)(9)  
Direct Project § 170.315(h)(1) or Direct Project, Edge Protocol, and XDR/XDM § 170.315(h)(2) |

* Red - New to the Base EHR Definition as compared to the 2014 Edition
** Privacy and security removed – now attached to the applicable certification criteria
Common Clinical Data Set

- Renamed the “Common MU Data Set.” This does not impact 2014 Edition certification.
- Includes key health data that should be accessible and available for exchange.
- Data must conform with specified vocabulary standards and code sets, as applicable.

<table>
<thead>
<tr>
<th>Patient name</th>
<th>Lab tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sex</td>
<td>Lab values/results</td>
</tr>
<tr>
<td>Date of birth</td>
<td>Vital signs (changed from proposed rule)</td>
</tr>
<tr>
<td>Race</td>
<td>Procedures</td>
</tr>
<tr>
<td>Ethnicity</td>
<td>Care team members</td>
</tr>
<tr>
<td>Preferred language</td>
<td>Immunizations</td>
</tr>
<tr>
<td>Problems</td>
<td>Unique device identifiers for implantable devices</td>
</tr>
<tr>
<td>Smoking Status</td>
<td>Assessment and plan of treatment</td>
</tr>
<tr>
<td>Medications</td>
<td>Goals</td>
</tr>
<tr>
<td>Medication allergies</td>
<td>Health concerns</td>
</tr>
</tbody>
</table>

**ONC INTEROPERABILITY ROADMAP GOAL**

2015-2017

Send, receive, find and use priority data domains to improve health and health quality

Red = New data added to data set (+ standards for immunizations)
Blue = Only new standards for data
## Certification Criteria

<table>
<thead>
<tr>
<th>Certification Criteria</th>
<th>What the Functionality Can Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation of social, psychological, and behavioral data (e.g., education level, stress, depression, alcohol use, sexual orientation and gender identity)</td>
<td>Allow providers and other stakeholders to better understand how these data can affect health, reduce disparities, and improve patient care and health equity</td>
</tr>
<tr>
<td>Exchange of sensitive health information (data segmentation for privacy)</td>
<td>Allow for the exchange of sensitive health information (e.g., behavioral health, substance abuse, genetic), in accordance with federal and state privacy laws, for more coordinated and efficient care across the continuum.</td>
</tr>
<tr>
<td>Accessibility of health IT</td>
<td>More transparency on the accessibility standards used in developing health IT</td>
</tr>
<tr>
<td>More granular recording and exchange of patient race and ethnicity</td>
<td>Allow providers to better understand health disparities based on race and ethnicity, and improve patient care and health equity.</td>
</tr>
</tbody>
</table>
## Certification Program Requirements*

### 2015 Edition Mandatory Certification Criteria
- Quality Management System - (g)(4)
- Accessibility-Centered Design - (g)(5)

### 2015 Edition Conditional Certification Criteria
- Amendments - (d)(4)
- Automatic Access Time-Out - (d)(5)
- Emergency Access - (d)(6)
- End-User Device Encryption - (d)(7)
- Integrity - (d)(8)
- Trusted Connection - (d)(9)
- Auditing Actions on Health Information - (d)(10)
- Safety Enhanced Design - (g)(3)
- Consolidated CDA Creation Performance - (g)(6)

### 2015 Edition Certification Criteria Associated with EHR Incentive Programs Stage 3

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Green Background</th>
<th>Red Font</th>
<th>Black Font</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication, Access Control, Authorization - (d)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditable Events and Tamper-Resistance - (d)(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Report(s) - (d)(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPOE – Medications - (a)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPOE – Laboratory - (a)(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPOE Diagnostic Imaging - (a)(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drug-Drug, Drug-Allergy Interaction Checks for CPOE - (a)(4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Demographics - (a)(5)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem List - (a)(6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medication List - (a)(7)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medication Allergy List - (a)(8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDS - (a)(9)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drug-Formulary and Preferred Drug List Checks - (a)(10)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smoking Status - (a)(11)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Family Health History - (a)(12)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient-Specific Education Resources - (a)(13)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implantable Device List - (a)(14)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transitions of Care - (b)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical Information Reconciliation and Incorporation - (b)(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Prescribing - (b)(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Export - (b)(6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Health Information Capture - (e)(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View, Download, and Transmit to 3rd Party - (e)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Messaging - (e)(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM – Report - (c)(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM – Record and Export - (c)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM – Import and Calculate - (c)(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM – Export and Calculate - (c)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM – Report - (c)(4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM – Import and Calculate - (c)(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM – Export and Calculate - (c)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CQM Filter - (c)(4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission to Immunization Registries - (f)(1)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission to PHA – Syndromic Surveillance - (f)(2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission to PHA – Reportable Laboratory Tests and Values/Results - (f)(3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission to PHA – Health Care Surveys - (f)(7)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission of Cancer Registries - (f)(4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission to PHA – Electronic Case Reporting - (f)(5)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission to PHA – Antimicrobial Use and Resistance Reporting - (f)(6)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**KEY:** Criteria are “new,” “unchanged,” “revised” as compared to the 2014 Edition

- **Green Background = new to the 2015 Edition**
- **Red Font = “unchanged” criteria (eligible for gap certification)**
- **Black Font = “revised” criteria**
Where have you seen Certified Health IT Provisions?

**Examples:**

- Medicare and Medicaid EHR Incentive Programs
- Physician Quality Reporting System (PQRS)
- Hospital Inpatient Quality Reporting (IQR)
- The Joint Commission for performance measurement initiative
- CPC alternate payment model and others
- Physician Self-Referral Law exception and Anti-kickback Statute safe harbor for certain EHR donations
- CMS chronic care management services (included in 2015 and 2016 Physician Fee Schedule rulemakings)
- Department of Defense Healthcare Management System Modernization Program
- HRSA Health Center Controlled Network Program

**CMS Quality Payment Program**

*Established by MACRA Act of 2015; Implemented by CMS in an Oct. 2016 Final Rule*
MACRA & the CMS Quality Payment Program: A Health IT Perspective

**Health IT in ACI**
- Closing the Health IT Referral Loop
- Bridging the Information Gap across Care Settings
- Incentivizes Public Health and Population Health Management
- Streamlining Reporting and Providing Flexibility

**Health IT in Quality**
- Seamless Information Exchange through Health IT
- Flexible Options for Electronic Reporting
- End-to-End Electronic Reporting Bonus

**Health IT in Improvement Activities**
- Includes a wide range of options that leverage certified health IT to support eligible clinicians in implementing clinical practice improvements.
- Certified EHR Technology Bonus for Improvement Activities

**Health IT In APMs**
- At least 50 percent of the clinicians in an Advanced APM must use certified EHR technology
- Other payer APMs will align with Medicare APMs using certified EHR technology in future years
- APM Entities must comply with HIPAA and may also include additional APM specific technology initiatives
The Advancing Care Information performance category includes measurement of eligible clinicians and groups use of certified EHR technology.

- **Protect Patient Health Information** (yes required)
- **Electronic Prescribing** (numerator/denominator)
- **Patient Electronic Access** (numerator/denominator)
- **Coordination of Care Through Patient Engagement** (numerator/denominator)
- **Health Information Exchange** (numerator/denominator)
- **Public Health and Clinical Data Registry Reporting** (yes required)
Clinicians must use certified EHR technology to report

For those using EHR Certified to the 2015 Edition:

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advancing Care Information Objectives and Measures</td>
<td>Combination of the two measure sets</td>
</tr>
</tbody>
</table>

For those using 2014 Certified EHR Technology:

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017 Advancing Care Information Transition Objectives and Measures</td>
<td>Combination of the two measure sets</td>
</tr>
</tbody>
</table>
Merit Based Incentive Program
Advancing Care Information Category

• Advances the goals of the HITECH Act to encourage the use of CEHRT and builds upon prior policies under Meaningful Use

• Scoring methodology emphasizes Patient Electronic Access, Coordination of Care Through Patient Engagement, and Health Information Exchange

• Reduced number of required measures from 11 -> 5 and improves upon prior “all or nothing” scoring

• Base reporting earns 50% credit; performance score based on the remaining optional measures

• Bonuses in ACI for completing certain Improvement Activities using CEHRT (e.g., providing 24/7 access, recording patient outcomes) and reporting to public health registries

• Hardship exemptions available
Merit Based Incentive Program
Advancing Care Information Category

ACI category weighted to zero for the following hardships:

- Lack of sufficient internet connectivity
- Extreme and uncontrollable circumstances (e.g., vendor issues)
- Lack of control over the availability of CEHRT
- No face-to-face interactions with patients
Section 106(b)(2) of the MACRA requires eligible providers to demonstrate that they have not knowingly and willfully limited or restricted the interoperability of certified EHR technology.

CMS finalized a new required attestation for health care providers using CEHRT in the EHR Incentive Programs and Merit Based Incentive Program (MIPS) to support the prevention of information blocking.
Quality Payment Program

Modernizing Medicare to provide better care and smarter spending for a healthier America.

qpp.cms.gov
Enhanced Oversight & Accountability Rule

Support greater accountability for health IT developers under the ONC Certification Program
• ONC Direct Review of Certified Health IT

• ONC-Authorized Testing Laboratories (ONC-ATLs)

• Transparency and Availability of Identifiable Surveillance Results
What is the EOA Final Rule?

- **Does not** create new certification criteria requirements for health IT developers
- **Does not** create new certification/health IT requirements for providers participating in HHS programs
- **Does not** establish a means for ONC to directly test and certify health IT (ONC-ACBs will continue to test and certify)
- **Does not** establish regular or routine auditing of certified health IT by ONC

- **Does** establish a regulatory process for ONC to directly review already certified health IT products
- **Does** increase ONC oversight of health IT testing bodies
- **Does** increase transparency and accountability by making identifiable surveillance results of certified health IT publicly available
• Support greater accountability for health IT developers under the Program

• Provide greater confidence to purchasers and users that health IT conforms to Program requirements when it is implemented, maintained, and used

• Sets up a process for ONC to work with health IT developers to remedy any identified non-conformities of certified health IT in a timely manner
With the vast majority of physicians and hospitals now using certified health IT, ONC plays an important role in helping ensure that these products operate safely and reliably in the field.

ONC direct review will:

- Be independent of (and may be in addition to) ONC-ACBs’ surveillance and other functions under the Program
- Focus on capabilities and aspects of health IT that are certified under the Program (i.e., “certified capabilities”), taking into consideration other relevant functionalities or products to the extent necessary to determine whether certified health IT is functioning in a manner consistent with Program requirements
- Focus on circumstances involving:
  1. Potential risks to public health or safety; or
  2. Practical challenges that may prevent ONC-ACBs from carrying out their surveillance responsibilities
ONC Direct Review of Certified Health IT

- **Serious Risk to Public Health or Safety**
  - ONC may initiate direct review if it has a reasonable belief that certified health IT may not conform to Program requirements because the certified health IT may be causing or contributing to conditions that present a serious risk to public health or safety.
  - ONC will consider:
    - The potential nature, severity, and extent of the suspected conditions;
    - The need for an immediate or coordinated government response; and
    - If applicable, information that calls into question the validity of the health IT’s certification or maintenance thereof under the Program.

- **Impediments to ONC-ACB Oversight**
  - ONC may initiate direct review if it has a reasonable belief that certified health IT may not conform to Program requirements and the suspected non-conformity presents issues that:
    - May require access to confidential or other information that is unavailable to an ONC-ACB;
    - May require concurrent or overlapping reviews by multiple ONC-ACBs; or
    - May exceed an ONC-ACB’s resources or expertise.

- **Examples – Six examples in the final rule (A through F (3-part example)) (81 FR 72420-25)**
• Establishes regulatory processes for ONC to have more direct oversight of testing labs under the Program. These processes are similar to the ONC-ACB processes.

• Provision enables ONC to oversee and address testing and certification performance issues throughout the entire continuum of the Program in an immediate, direct, and precise manner, including by:
  
  » Authorizing testing labs as ONC-ATLs.
  
      – Does not require labs applying for ONC-ATL status to obtain additional accreditation beyond NVLAP accreditation for health IT testing
  
  » Specifying requirements for retaining ONC-ATL status and means for ONC to suspend and revoke ONC-ATL status under the Program.
Comparison of ONC-ATL and ONC-ACB Processes

Current ONC-ACB Process
- Entity accredited by ONC-Approved Accreditor (ONC-AA)
- Entity applies to NC to operate within the Program
- Authorization by NC to operate within the Program

Same violations/revocation processes

Finalized ONC-ATL Process
- Entity accredited by NVLAP
- Entity applies to NC to operate within the Program
- Authorization by NC to operate within the Program

NOTE: Distinct PoPC for ATLs (§ 170.524)
Before this rule, ONC only lists corrective action plans for non-conformities found by ONC-ACBs on the CHPL. Through this final rule, ONC will provide more complete information that illuminates good performance and continued conformity with Program requirements for certified health IT.

- Requires ONC-ACBs to make identifiable surveillance results publicly available on the web-based Certified Health IT Product List (CHPL) on a quarterly basis.

- Further enhances transparency and provide customers and users of certified health IT with valuable information about the overall conformity of certified health IT to Program requirements.
Snapshot of Office of Policy Initiatives

- Model Privacy Notice
- EHR Contract Guide
- Public Health - Zika Response
- Patient Generated Health Data
- Patient Access Resources
There is now a broad range of consumer health technologies beyond PHRs.

More and more individuals are obtaining access to their electronic health information and using consumer health technology to manage this information.

Users are concerned about privacy and security of their data.

Existing privacy policies can be long, complex, and confusing.

Not all users read the privacy policy and those that do may not fully understand the content in the policy.

What if...

... Privacy practices were as easy to understand as a nutrition label?

... Users were provided with a snapshot of the privacy practices that they are most concerned about in terms that they understand?
Model Privacy Notice (MPN): a voluntary, openly available resource designed to help developers provide transparent notice to consumers about what happens to their data.

The MPN’s approach is to provide a standardized, easy-to-use framework to help developers clearly convey information about privacy and security to their users.

The 2011 version of the MPN was developed in collaboration with the Federal Trade Commission and focused on Personal Health Records (PHRs), which were the emerging technology at the time.
2016 Model Privacy Notice

Draft Preamble

As of December 2, 2016

The Model Privacy Notice (MPN) is a voluntary, openly available resource designed to help health technology developers provide transparent notice to consumers about what happens to their digital health data when the consumer uses the developer’s product. The MPN’s approach is to provide a standardized, easy-to-use framework to help developers clearly convey information about privacy and security to their users. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies.

The Office of the National Coordinator for Health Information Technology (ONC) is updating the 2011 version of the MPN. The 2011 version focused on personal health records (PHRs), which were the emerging technology at the time. The health information technology market has changed significantly in the last five years and there is now a larger variety of products such as exercise trackers, wearable health technologies, or mobile applications that help individuals monitor various body measurements. As such, it is increasingly important for consumers to be aware of health technology developers’ privacy and security policies, including data sharing practices.

<table>
<thead>
<tr>
<th>Preamble for Health Technology Developers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is the Model Privacy Notice (MPN)?</strong></td>
</tr>
<tr>
<td><strong>Who is the MPN for?</strong></td>
</tr>
<tr>
<td><strong>What laws might apply to you?</strong></td>
</tr>
<tr>
<td><strong>Does use of this MPN satisfy HIPAA requirements to provide a notice of privacy practices?</strong></td>
</tr>
</tbody>
</table>

---

Draft Content

As of December 2, 2016

Note: Developers of consumer health technology or apps (‘‘health technology developers’’) that collect digital health data about individuals would use this template to disclose to consumers the developer’s privacy and security policies. ‘‘We’’ refers to the health technology developer or technology product and ‘‘you/your’’ refers to the user/consumer of the health technology. For all endnotes provided in the MPN, the information specified in the endnote is required to be included in the privacy notice. However, for purposes of the Challenge, flexibility is permitted for how the information is presented (e.g., use of a link or pop up box) as long as the format maintains clear interfaces.

*Directions for the health technology developer: If the health technology developer is a HIPAA covered entity, select one of the following statements to be inserted in the privacy notice:

**Option 1:** Please note that the health data we collect as part of this [insert name of technology product] are not protected by HIPAA and our company’s HIPAA Notice of Privacy Practices does not apply.

**Option 2:** Some of the health data we collect as part of this [insert name of technology product] are also protected by HIPAA. Read our HIPAA Notice of Privacy Practices [embed link or popup] for more information.

---

**Use: How we use your data internally**

- To provide the primary service of the app or technology
- To develop marketing materials for our products
- To conduct scientific research
- For company operations (e.g., quality control or fraud detection)
- To develop and improve new and current products and services (e.g., analytics)
- Other:

**Share: How we share your data externally with other companies or entities**

- We share your **identifiable data**:
  - To provide the primary service of the app or technology
  - To conduct scientific research
  - For company operations (e.g., quality control or fraud detection)
  - To develop and improve new and current products and services (e.g., analytics)
  - Other:
  - **We DO NOT share your identifiable data**

- We share your **data AFTER removing identifiers** (note that remaining data may not be anonymous):
  - For the primary purposes of the app or technology
  - To conduct scientific research
  - For company operations (e.g., quality control, fraud detection)
  - To develop and improve new and current products and services (e.g., analytics)
  - Other:
  - **We DO NOT share your data after removing identifiers**
### ONC’S 2016 Model Privacy Notice (MPN)

#### Sell: Who we sell your data to

<table>
<thead>
<tr>
<th>We sell your identifiable data to data brokers, marketing, advertising networks, or analytics firms.</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes; only with your permission</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>We sell your data AFTER removing identifiers (note that remaining data may not be anonymous) to data brokers, marketing, advertising networks, or analytics firms.</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes; only with your permission</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Store: How we store your data

<table>
<thead>
<tr>
<th>Are your data stored on the device?</th>
<th>Yes / No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are your data stored outside the device at our company or through a third party?</td>
<td>Yes / No</td>
</tr>
</tbody>
</table>

#### Encryption: How we encrypt your data

<table>
<thead>
<tr>
<th>Does the app or technology use encryption to...</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>encrypt your data in the device or app?</td>
<td>Yes, by default</td>
<td></td>
</tr>
<tr>
<td>Yes, when you take certain steps (click to learn how)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>encrypt your data when stored on our company servers or with an outside cloud computing services provider?</th>
<th>Yes, by default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, when you take certain steps (click to learn how)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>encrypt your data while it is transmitted?</th>
<th>Yes, by default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, when you take certain steps (click to learn how)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Policy Changes: How we will notify you if our privacy policy changes

Describe how/if the company will notify consumers of privacy policy changes (e.g., merger or acquisition) and provide link to section in privacy policy.

#### Breach: How we will notify you and protect your data in case of an improper disclosure

(Company name) complies with all applicable laws regarding breaches. Describe how the company will protect consumers’ data in case of a breach and provide link to section in privacy policy.

#### Contact Us

- [Legal Entity Name]
- [Link to full privacy policy]
- [Link to Online Comment/Contact Form]
- [Email Address]
- [Phone Number]
- [Address; minimum, Country]

---

1 Health data can include, but is not limited to: wellness information (e.g., exercise or fitness habits, nutrition, or sleep data), health markers (e.g., blood pressure, BMI, or glucose), information on physical or mental health conditions, insurance or health care information, or information that integrates into or receives information from a personal health record.

2 Include definition of “identifiable data.” Identifiable data means: data, such as your name, phone number, email, address, health services, information on your physical or mental health conditions, or your social security number, that can be used on its own or with other information to identify you.

3 If unclear, specify what the developer considers the primary service.

4 Include definition of “analytics.” Analytics means: the process of examining data to draw conclusions from that information. Alternatively, a more consumer friendly definition may be substituted as a result of the Challenge, including based on consumer testing feedback.

5 Include definition of “identifiable data.” Identifiable data means: data, such as your name, phone number, email, address, health services, information on your physical or mental health conditions, or your social security number, that can be used on its own or with other information to identify you.

6 If unclear, specify what the developer considers the primary service.
ONC put out a request for information on March 1, 2016 and sought comment on what information practices health technology developers should disclose to consumers and what language should be used to describe those practices.

Further engage stakeholders, including our federal advisory committees, federal partners, privacy organizations, developers and developer associations, and, of course, consumers

An updated MPN

“Privacy Policy Snapshot” Challenge
The Privacy Policy Snapshot Challenge calls upon developers, designers, health data privacy experts, and creative, out-of-the-box thinkers to use ONC’s Model Privacy Notice template to create an online tool that can generate a user-friendly “snapshot” of a product’s privacy practices.

ONC will award a total of $35,000 in prizes through this challenge.

The deadline for submission is April 10, 2017 with winners expected to be announced in mid-2017. Submissions can be entered here.

The Federal Register Notice announcing the challenge can be viewed here.

For more information on the MPN, please visit: https://www.healthit.gov/policy-researchers-implementers/model-privacy-notice-mpn
The EHR Contract Guide should not be construed as legal advice and does not address all possible legal and other issues that may arise with the acquisition of an electronic health record or other health information technology product or service. Each health care provider organization is unique and will need to consider its particular circumstances and requirements, which cannot be contemplated or addressed in this guide. A health care provider organization should obtain the advice of an experienced attorney whenever it proposes to enter into a legally binding contract.
Helps Health IT Purchasers:

- Understand the “fine print”
- Consider contract provisions that impact whether the technology they are contracting for will meet their needs and expectations
- Ask the right questions when selecting an EHR and better communicate their requirements to potential vendors
- Consider and manage expectations and offer a framework for negotiating reasonable contract terms that reflect best practice contracting principles
Part A: The Importance of Planning: Putting Your Best Foot Forward

• Highlights the critical planning steps that providers should take to properly understand and communicate their requirements to potential vendors. Areas addressed include:
  » Types of EHR products and service models
  » Researching and comparing EHR products and vendors
  » Identifying and prioritizing technical and operational requirements
  » Understanding certification and regulatory requirements
  » Procurement strategy, planning and resourcing
Part B: Negotiating EHR Contracts: Key Terms and Considerations for Providers

- Focuses on the negotiation and contracting phase of acquiring an EHR
- Contains strategies and recommendations for negotiating best practice EHR contract terms
- Addresses the practical issues important to providers
- Illustrates how legal issues might be addressed in a contract by providing example contract language
• Working with Public health specialists, health IT stakeholders and industry

• Federal Advisory Committee - Public Health Task Force (Pregnancy Status)

• Community of Practice - Designed to build a communication pathway between the public health and health IT developer communities to identify and share promising practices around public health

• Zika Response Support
  » ONC/CMS Health IT- Focused Webinars with stakeholders on Zika response
  » Build on lessons learned from Ebola, MERS & H1N1
  » Algorithm for developers (clinical decision support)
  » Create vocabulary sets to support Zika-related terminology
### Patient-generated health data (PGHD) are health-related data created, recorded, or gathered by or from patients (or family members or other caregivers) to help address a health concern.

#### PGHD include, but are not limited to:

- **Health history**
- **Treatment history**
- **Biometric data**
- **Symptoms**
- **Lifestyle choices**

#### PGHD are distinct from data generated in clinical settings and through encounters with providers in two important ways:

- **Patients**, not providers, are **primarily responsible for capturing** or recording these **data**.
- **Patients** decide how to **share** or distribute these **data to** health care **providers** and others.
• **Draft White Paper**
  » Developed by Accenture Federal Services
t  » Draft white paper considers best practices, gaps, and opportunities for progress in the collection and use of PGHD for research and care delivery through the year 2024
  » Available for review at:
    https://www.healthit.gov/sites/default/files/

• **Pilot Demonstrations**
  » The concepts in the draft white paper will be tested and refined through real world application in pilot demonstrations
  » The results will inform updates to the white paper at the end of the two-year project
  » Accenture Federal Services has established two pilot demonstrations with:
    – TapCloud in partnership with Amita Health
    – Validic in partnership with Sutter Health
AVAILABLE ONLINE AT WWW.HHS.GOV/HIPAA

Fact Sheet
Scope FAQs
Form and Format and Manner of Access FAQs
Timeliness FAQs
Other (Clinical Labs) FAQs