# Patient Requested Restrictions Certification Criteria

Elisabeth Myers, ONC

# Disclaimers and Public Comment Guidance

- The materials contained in this presentation are based on the proposals in the "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing“ proposed rule. While every effort has been made to ensure the accuracy of this restatement of those proposals, this presentation is not a legal document. The official proposals are contained in the proposed rule.

- ONC must protect the rulemaking process and comply with the Administrative Procedure Act. During the rulemaking process, ONC can only present the information that is in the proposed rule as it is contained in the proposed rule. ONC cannot interpret that information, nor clarify or provide any further guidance.

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

# NEW Patient Requested Restrictions Criterion in § 170.315(d)(14)

## Proposal

- ONC proposes that for any data expressed in the standard in § 170.213, a health IT developer must enable a user to flag whether such data needs to be restricted from being subsequently used or disclosed and prevent any data flagged from being included in a use or disclosure
- ONC proposes to modify the Privacy and Security Framework in § 170.550(h) to add the proposed new "patient requested restrictions" criterion and to require it by January 1, 2026 (or 24 months after the effective date of a final rule)
- ONC also proposes to modify § 170.315(e)(1) to add a paragraph (iii) stating patients (and their authorized representatives) must be able to use an internet-based method to request a restriction to be applied for any data expressed in § 170.213

## Benefits

As ONC pursues policies intended to improve the interoperability and sharing of data through adoption of standards-based certification criteria and implementation specifications, we are aware of the imperative to protect health data privacy. We are also cognizant that the concept of "sensitive data" is dynamic and specific to the individual. This proposal would:

- Enable a user of certified health IT to implement a process to restrict data from use or disclosure in response to a patient request
- Support the HIPAA Privacy Rule's "right to request a restriction" on uses and disclosures (See 45 CFR 164.522(a))
- Advance health IT tools to support patient-directed privacy requests for data the patient deems sensitive (e.g., through a patient portal)

# Patient Requested Restrictions Criterion in § 170.315(d)(14) - Primary Proposal

- “Enabl[ing] a user to flag” means enabling the user of the Health IT Module to indicate that a request for restriction was made by the patient and that the user intends to honor the request
  - That request made by the patient could be in part automated for requests made through an internet-based method, however, the functionality under the proposed new criterion in § 170.315(d)(14) must include the ability for the user to indicate a request made via other means
- The health IT developer would have the flexibility to implement the “enable a user to flag” functionality in the manner that works best for their users and systems integration expectations

# Standards Agnostic Approach of the Primary Proposal

- The developer of a certified Health IT Module would have the flexibility to implement the restriction on the inclusion in a subsequent use or disclosure via a wide range of potential means dependent on their specific development and implementation constraints
  - e.g., flagged data would not be included as part of a summary care record, not be displayed in a patient portal, or not be shared via an API
- Such “flags” may leverage use of security labels like those included in the HL7 data segmentation for privacy (DS4P) implementation guides (IGs), or other data standards such as provenance or digital signature specifications.
  - The use of such standards or specifications would be at the discretion of the health IT developer.
- We believe this approach would provide flexibility for developers of certified health IT to provide this functionality in ways that are convenient for their underlying system structures and in support of existing workflows for patient requested restrictions under the HIPAA Privacy Rule.

# Alignment with Adopted Standards – Alternate Proposals and Requests for Information

- We propose and seek comment on a set of alternate proposals that propose § 170.314(d)(14) reference specific standards rather than proposing it be standards agnostic
- We seek comment on a set of alternate proposals which would instead reference the HL7 CDA DS4P IG and the HL7 FHIR DS4P IG and which consider the potential to adopt these standards with constraints
- Specifically, the alternative proposals are as follows and we seek comment on:
  - a set of alternate proposals adopting each of the HL7 DS4P IGs, the HCS Security Label Vocabulary, or both for the new criterion in § 170.315(d)(14)
  - alternate proposals adopting the HL7 DS4P IGs and/or the HCS Security Label Vocabularies with constraints beyond those described in the IGs, that, if finalized, would constrain the requirements within the IGs to only certain use cases
  - an additional alternate proposal that, if finalized, would limit the specified scope of USCDI data that the proposed new criterion in § 170.315(d)(14) and the proposed revised criterion in § 170.315(e)(1) would be required to support

# Alternative Approach Proposals Considerations

- Alternative approach — proposing that § 170.314(d)(14) reference specific standards rather than proposing it be standards agnostic — would remove ambiguities inherent in the standards agnostic proposal by establishing a basis for the “flag” on the data using consensus standards for security labeling
  - The use of these standards may also facilitate implementation of capabilities to support patient requested restrictions on certain uses or disclosures by providing taxonomy for the scope of such restrictions and the purpose or use to which such restrictions apply
  - We believe the alternative proposals, which rely on HL7 standards, may be preferrable for developers of certified health IT that seek standards-based implementation guidance over flexibility

# Alignment with Applicable Law – Request for Information

- Our intent for proposing a technical means for patients to request a restriction on their data is to advance tools that support privacy laws, including the HIPAA Privacy Rule right to request a restriction of certain uses and disclosures*

- Use of any future Health IT Module certified to these proposed requirements would not, by itself, fully discharge the obligations under the HIPAA Privacy Rule of a covered entity to allow an individual to request a restriction on the use or disclosure of their PHI for treatment, payment, or health care operations or to have policies in place by which to accept or deny such requests
  - Use of any such certified Health IT Module would not discharge the obligations of a covered entity to meet any other requirements under 45 CFR 164.522
  - In addition, there may be other applicable laws that affect the exchange of particular information, and those laws should be considered when developing individual choice policies

- We seek comment on whether there are modifications, adjustments, additions, or restrictions we should consider for our proposal to better support privacy workflows under the HIPAA Privacy Rule

* HHS Office for Civil Rights. HIPAA "Right to Request a Restriction": https://www.hhs.gov/hipaa/for-professionals/faq/right-to-request-a-restriction/index.html.

ONC | HealthIT ADVISORY COMMITTEE

# Thank you.

**Phone:** 202-690-7151

**Health IT Feedback Form:** https://www.healthit.gov/form/healthit-feedback-form

**Twitter:** @onc_healthIT

**LinkedIn:** Office of the National Coordinator for Health Information Technology

**Youtube:** https://www.youtube.com/user/HHSONC

HealthIT.gov

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