

## ILHIE Authority Data Security and Privacy Committee

### Briefing Summary: Panel #6 – Current and Future Technologies – Patient Matching

- Should the state-level ILHIE utilize a unique patient identifier for the purpose of matching patient records?
- To what extent should the state-level ILHIE impose upon providers connected to the state-level ILHIE standards for the degree of patient matching accuracy achieved in provider systems?

### Federal Guidance

- The Federal HIPAA Privacy Rule currently does not specifically address the accuracy of patient matching.
- Proposals to create a Federal unique patient identification number for each U.S. resident for use in health care data patient matching have been opposed by Congress.
- ONC recently issued guidance to the recipients of HIE planning grants that HIEs “should implement strategies and approaches to ensure... that patients are correctly matched with their data.”
  - In its reply to the ONC, OHIT indicated that it considered such a requirement as “reasonable”, but noted the following concerns:
    - Patient Matching. Matching by an HIE of a specific individual to someone else’s clinical data is a serious problem that the HIE will wish to investigate and rectify; patient clinical data overlays, potentially resulting in clinical decisions based on the wrong data, can present a serious treatment risk to the patient. Such errors may arise because of patient identity theft and subsequent erroneous entries on the patient’s record, or from mismatches arising from a provider’s Master Patient Index (MPI) (or functionally equivalent computational patient matching method). To reduce its exposure to potential liability the HIE will wish to address erroneous matching. To effectively investigate and rectify such errors, a collaborative approach involving the relevant data custodians would need to be established.
    - Downstream MPI accuracy. The accuracy of the State-level Master Patient Index (MPI) will depend in part on the proper maintenance by sub-State RHIOs of their respective MPIs which interface with the State-level MPI. To effectively investigate and rectify patient matching errors, a collaborative approach involving the relevant data custodians would need to be established.

*Policy Option 1: ILHIE directed to implement Unique Patient Identifier for the ILHIE MPI.*

*Policy Option 2: ILHIE given discretion to implement Unique Patient Identifier for the ILHIE MPI if operationally necessary or desirable.*

*Policy Option 3: ILHIE directed NOT to implement Unique Patient Identifier for the ILHIE MPI*

## ILHIE Authority Data Security and Privacy Committee

### Briefing Summary: Panel #6 – Current and Future Technologies – Patient Data Access and Correction

- To what extent should the State-level HIE grant patients the right to request access to a copy of their records and to request corrections, arguably in duplication of existing federal patient rights with respect to records in the custody of providers?
- If inaccuracies are apparent, should the HIE address patient requests to correct data or refer such requests to the patient’s healthcare providers?

#### Federal Guidance: Patient Access

- The Federal HIPAA Privacy Rule currently provides patients a right of access to information at the covered entity (provider, health plan) level;<sup>1</sup> HIPAA currently does not provide patients a right to access information directly from HIEs. Individuals are entitled under HIPAA to review and obtain a copy of their protected health information in a covered entity’s “designated record set”<sup>2</sup>, except in certain circumstances. Certain data is excluded.<sup>3</sup> For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. For certain denials, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.<sup>4</sup> Covered entities must (1) respond to requests for access in a timely manner (30 – 60 days); (2) develop and implement reasonable policies and procedures to verify the identity and authority of any person who requests PHI; and (3) provide access to the PHI in the form or format requested by the individual, if it is readily producible. Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.
- ONC recently issued guidance that “Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information (IIHI) in a readable form and format...HIE entities should make concrete plans to give patients electronic access to their compiled IIHI...”

---

<sup>1</sup> 45 CFR §164.524.

<sup>2</sup> The “designated record set” is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider’s medical and billing records about individuals or a health plan’s enrollment, payment, claims adjudication, and case or medical management record systems. 45 CFR §164.501.

<sup>3</sup> HIPAA excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories.

<sup>4</sup> A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. §552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 CFR §164.524.

## ILHIE Authority Data Security and Privacy Committee

### Briefing Summary: Panel #6 – Current and Future Technologies – Patient Data Access and Correction

- In its reply to the ONC, OHIT indicated that it considered such a requirement as “futuristic”. OHIT noted the following concerns:
- Denial of Access. As noted above, a patient’s right to demand from a provider access to data is not unconditional; under current HIPAA a provider can reject a data access request if in the provider’s judgment a disclosure may cause someone harm or compromise ongoing medical research. Such a determination presumably requires knowledge of relevant facts related to the demographic and clinical information contained in the patient record and the context of the request, and is presumably triggered in response to an access request. Applying a similar conditional access principle to data access from an HIE, the HIE would presumably lack sufficient knowledge needed to deny access requests. Even if the HIE were to acquire the ability to analyze the clinical content of a patient record and appreciate the relevant context of the access request, the HIE does not have a professional clinical treatment relationship to any party nor professional responsibilities which are enforced by licensing and disciplinary authorities. It is arguably undesirable, and potentially dangerous, to place responsibilities upon the HIE requiring the discretionary exercise of clinical judgment. The additional risk that the HIE would assume of liability arising from unfortunate decisions would be difficult to quantify and insure against.
- Inconsistent Rulings. The prospect of the HIE and a data custodian reaching inconsistent discretionary decisions in response to patient access requests is undesirable.
- Patient Identification. Providers with a treatment relationship with a patient presumably possess demographic and other information which enables them to reasonably verify the identity of an individual seeking access to data. The ability of an HIE, removed from the point of care, to verify the identity of an individual electronically seeking access to data “may be tricky”.<sup>5</sup> The ability of patients in the State of Illinois to obtain a digital ID/certificate<sup>6</sup> may provide a potential solution.

### Federal Guidance: Patient Data Correction

- The Federal HIPAA Privacy Rule currently provides patients the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete.<sup>7</sup> (Since HIEs are not covered entities, HIPAA currently does not provide patients a right to request HIEs to correct patient information.) If a covered entity accepts an amendment request, it must make reasonable efforts to

---

<sup>5</sup> Noam Arzt, “Privacy and SecurityCoP, Privacy and Security Framework: Technical model distinctions and key considerations”, March 29, 2012, slide 8.

<sup>6</sup> See <http://www2.illinois.gov/pki/Pages/default.aspx>.

<sup>7</sup> 45 CFR §164.526.

## ILHIE Authority Data Security and Privacy Committee

### Briefing Summary: Panel #6 – Current and Future Technologies – Patient Data Access and Correction

provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.<sup>8</sup> If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record, to be provided "with any future disclosures" of the disputed information. The Rule specifies processes for requesting and responding to a request for amendment, including a patient right to appeal a denial decision to the covered entity and to the Secretary of HHS. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.

- ONC recently issued guidance that "Individuals should be provided with a timely means to dispute the accuracy or integrity of their IHI, and to have erroneous information corrected or to have a dispute documented if their requests are denied... HIE entities should... develop clearly defined processes (1) for individuals to request corrections to their IHI and (2) to resolve disputes about information accuracy and document when requests are denied."
  - In its reply to the ONC, OHIT indicated that it considered such a requirement as "futuristic". OHIT noted the following concerns:
    - Denial of Correction. As noted above, a patient's right to demand from a provider correction to data is not unconditional; under current HIPAA a provider can reject a data correction request if the provider did not create the information or if in the provider's judgment the patient's record is "accurate and complete".<sup>9</sup> Such a determination presumably requires knowledge of relevant facts related to the demographic and clinical information contained in the patient record and the context of the request. Applying a similar conditional correction principle to data correction by an HIE, the HIE did not create the clinical information and otherwise would presumably lack the sufficient knowledge needed to assess correction requests for potential denial. Even if the HIE were to acquire the ability to analyze the clinical content of a patient record and appreciate the relevant context of the correction request, the HIE does not have a professional clinical treatment relationship to any party nor professional responsibilities which are enforced by licensing and disciplinary authorities. It is arguably undesirable, and potentially dangerous, to place responsibilities upon the HIE requiring the discretionary exercise of clinical judgment. The additional risk that the HIE would assume of liability arising from unfortunate decisions would be difficult to quantify and insure against.

---

<sup>8</sup> Covered entities may deny an individual's request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 45 CFR §164.526(a)(2).

<sup>9</sup> 45 CFR §164.526(a). Applying the authorship principle, an HIE should only correct data the HIE created.

## ILHIE Authority Data Security and Privacy Committee

### Briefing Summary: Panel #6 – Current and Future Technologies – Patient Data Access and Correction

- Patient Statement of Disagreement. The patient will apparently be entitled to “have a dispute documented” if a correction request is denied by the HIE; assuming the current HIPAA requirements would be applied at the HIE level, the patient would have the right to submit a written statement disagreeing with a correction request denial, which would need to be distributed with all future transmissions of the disputed data. In the event that an HIE does not control or maintain the disputed data, or assembles and transmits only discrete data elements from a designated record set (such as for a CCD/CCR/C32 continuity of care document), it is difficult to envision how an HIE would operationalize the required future distribution of the patient’s statement of disagreement.
- Distribution of Corrections. If a correction is accepted by the HIE, the distribution of the correction by the HIE to all recipients of the erroneous data could be operationally challenging.
- Dispute Resolution. As noted above, in the event a provider denies a patient’s data correction request, the patient enjoys certain appeal rights (to the provider entity and the Secretary of HHS). To additionally place the HIE in the middle of a patient dispute with a provider with the task of resolving the dispute, requires of the HIE dispute resolutions capabilities and processes that few HIEs possess or have envisioned.
- Inconsistent Rulings. The prospect of the HIE and a data custodian reaching inconsistent decisions in response to patient data correction requests is undesirable.

#### **Policy Options: patient access to data at HIE**

*Policy Option 1a: HIE refers patient to data custodians holding patient PHI; each custodian exercises discretion over PHI it holds.*

*Policy Option 1b: on behalf of patient, HIE queries each data custodians holding patient PHI; each custodian exercises discretion over PHI it holds. HIE aggregates and applies discretionary decisions of data custodians, and provides patient access to PHI data.*

*Policy Option 1c: HIE creates own panel of clinicians to exercise discretion re: release of PHI data to patient.*

#### **Policy Options: patient correction of data through HIE**

*Policy Option 2a: HIE refers patient to data custodians holding patient PHI; each custodian exercises discretion over PHI it holds.*

## ILHIE Authority Data Security and Privacy Committee

### **Briefing Summary: Panel #6 – Current and Future Technologies – Patient Data Access and Correction**

*Policy Option 2b: on behalf of patient, HIE queries each data custodians holding patient PHI; each custodian exercises discretion over PHI it holds, corrects PHI data in its custody.*

*Policy Option 2c: HIE creates own panel of clinicians to exercise discretion re: correction of PHI data.*

*Policy Option 2c1: HIE demands correction of PHI data at custodian source*

*Policy Option 2c2: HIE appends special notice regarding suspect PHI data*

*Policy Option 2c3: HIE implements special procedures to address medical identity theft*