

Principles as applied to Directed Exchange Between Health Care Entities

1. **Individual access: individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format. Policy expectation: should be easy (ideally for both provider and individual) and available at reasonable cost.**

Health Information Technology (HITECH) requires electronic health record (EHR) users to provide individuals with electronic copy if requested (labor costs only) (some state law limits may apply); meaningful use proposed rule included particular individual access requirements. An individual's right to access a provider's record with a provider includes information obtained from other sources if it is incorporated into that provider's record.

Questions to resolve/Recommendations:

- To the extent that an *intermediary* retains personal health information (PHI), subject to any state laws, an individual should have a right to access that intermediary's record.
- Provider is responsible for ensuring that information is sent to the right patient—but additional work is needed to assist providers with identification/authentication. Suggest creating a subcommittee to develop 2-3 options for the Tiger Team to consider in July.

2. **Correction – Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.**

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule currently sets forth correction/amendment process.

Questions to Resolve/Recommendations:

- Providers should establish a process for responding to individual inquiries about correction of the record (doesn't need to be extensive – we just want them to think in advance about how they will respond, since these requests will occur more often). Providers also need education on current legal requirements re: correction, and HHS should provide guidance to providers on how to set up a dispute resolution/correction process.
- Who is responsible for correcting information received from another source? In other words, if Provider A makes available information

received from Provider B, and if a patient claims Provider B's data is inaccurate, who makes the correction and how?

Proposed answer: Provider B can, at their option, tell the patient that the information came from Provider A, and the patient needs to contact Provider A to get the information corrected.

[Here is an example of why this approach might be a good idea. Dr. B admits a patient to the hospital and sends a record indicating that the patient is allergic to Penicillin. The patient informs the hospital, however, that he/she is not allergic. The hospital, at their option, can tell the patient that he/she should contact Dr. B to get the record corrected. When the patient contacts Dr. B, the physician informs the patient that he/she really is allergic to Penicillin, but knows that drug by another name.]

- Recommended best practice: EHRs show the source of the information when it is presented.

3. **Data quality and integrity – persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.**

Questions to Resolve/Recommendations:

- Provider sending information represents at time of transmission that the data is an accurate representation of what is in the provider's record about the right patient and is sent from a system that includes appropriate security controls (as required by Interim Final Rule (IFR) or recommended for Directed Exchange).
- See our recommendations for Directed Exchange (including verification of both source and destination, such as through use of a digital certificate).

4. **Openness and Transparency - there should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.**

HIPAA Privacy Rule requires providers to provide "HIPAA Notice" (not always well understood and doesn't necessarily address new environment).

Questions to Resolve/Recommendations:

- Department of Health and Human Service/Extension Centers should develop guidance to help providers educate their patients about EHRs and electronic health information exchange.
- Office for Civil Rights (OCR) should make clear in guidance that this is part of HIPAA notice requirement.
- Intermediaries should be required to be transparent to providers about what they do with data (protected health information, PHI, and de-identified data).

5. Individual Choice (Individual Participation and Control) – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.

HIPAA does not require consent for treatment, payment, and health care operations (TPO) disclosures but authorization is required in certain circumstances; Part 2 regulations require consent to disclose identifiable health information related to substance abuse treatment; state laws require consent.

Questions to Resolve/Recommendations:

- No additional consent should be required (beyond current law) for directed exchange to meet meaningful use stage 1 if (1) directed exchange occurs using the encryption requirements described in the IFR; (2) the parties comply with the Directed Exchange Recommendations; (3) the intermediaries, if any, do not reuse data or make PHI available to other organizations.

6. Collection, use and disclosure limitation—individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified lawful purpose(s) and never to discriminate inappropriately.

HIPAA Privacy Rule includes minimum necessary standard, which applies to access, use and disclosure of PHI but not necessarily collection. OCR is required to issue guidance on minimum necessary; limited data set can be used to comply.

Questions to Resolve/Recommendations:

- See other Directed Exchange recommendations with respect to Intermediary access to PHI.

7. **Safeguards – individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use or disclosure.**

HIPAA Security Rule requires this; certification IFR requires that systems have certain capabilities (including encryption, audit trails).

Questions to Resolve/Recommendations:

- See other Directed Exchange recommendations.

8. **Accountability/Oversight/Enforcement/Remedies—These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.**

HIPAA privacy and security rule includes enforcement mechanisms; HITECH also increased penalties, vested additional enforcement authority with state AGs, and made business associates directly accountable.

Questions to Resolve/Recommendations:

- See other Directed Exchange recommendations re: federal and state governments playing a role in establishing trusted credentialing, business associate agreements as at least one potential tool for enforcing requirements against intermediaries.