

ILHIE Authority Data Security and Privacy Committee

Briefing Summary: Panel #4 – Fostering Public Trust in Health Information Exchanges – Enforcement and Mitigation Strategies

If patients do not trust HIEs due to actual or perceived risks they may chose not to have their personal health data available through the HIE.

- Because an HIE's success is directly related to patient participation, what sort of mechanisms should be in place to foster public trust in HIEs?
- What sort of enforcement monitoring is most practical?
 - Breach reporting?
 - Real time network monitoring?
 - Field monitoring?
 - Or a combination of all three?
- If a breach does occur, what are the proper strategies for breach mitigation?
- What is the best way to show the public that these mechanisms and strategies are in place to protect patient data?

Briefing Summary: Panel #7 – Protecting Patient Data: Security Compliance Standards for Health Information Exchanges

Protecting patients' privacy and securing their health information is imperative to building patient trust, which is a requirement to realizing the full potential of HIEs.

- To build trust by protecting patient data, what restrictions should there be on permitted uses of data by HIEs?
- Which entity or entities should establish and impose security compliance standards on HIEs?
- Should ILHIE impose such standards on sub-State HIEs?