

ILHIE Privacy & Patient Consent Preferences

Ivan Handler, CTO ILHIE



- Initial ILHIE Authority policy
 - Meaningful Disclosure
 - Opt-out flag and procedures
 - Introduction to consent granularity
- Security Breach scenarios and considerations
 - Breach scenarios
 - How ILHIE protects data
 - ILHIE recommendations on data protection
- SHARPS presentation by Dr. Carl Gunter

- Patients have the right to opt-out of ILHIE
 - That is not allow their information to be transferred via ILHIE
- Providers must present patients with their options
 - For the disclosure of their data electronically
 - Information on health information exchange
 - Opportunity to opt-out

MPI

- Master Patient Index
- Cross reference
- Used to identify patients

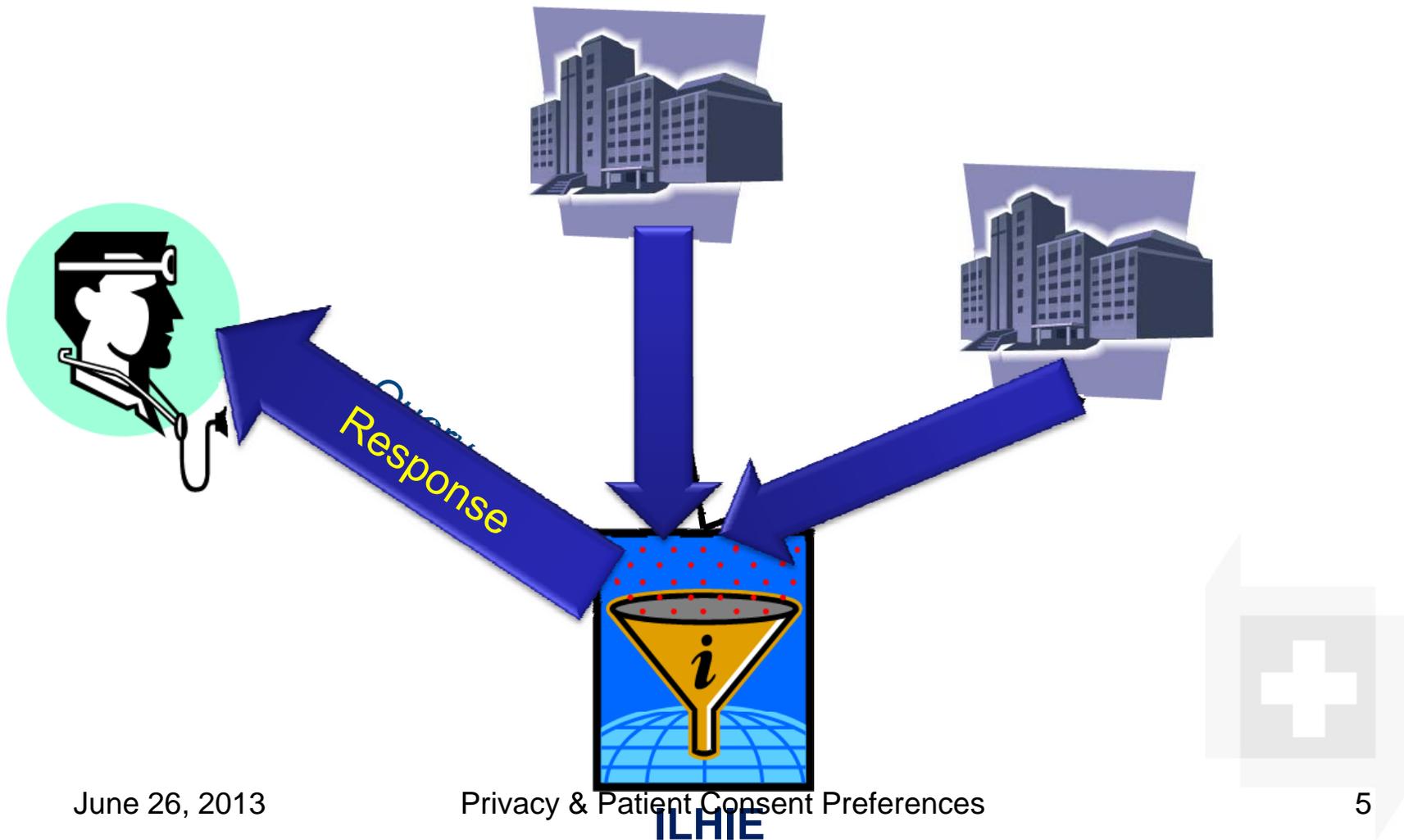
HPD

- Provider Directory
- Used to identify providers
- Can be used for Direct addressing

RLS

- Record Locator Service
- Discovers records for a patient
- Returns aggregate record to provider

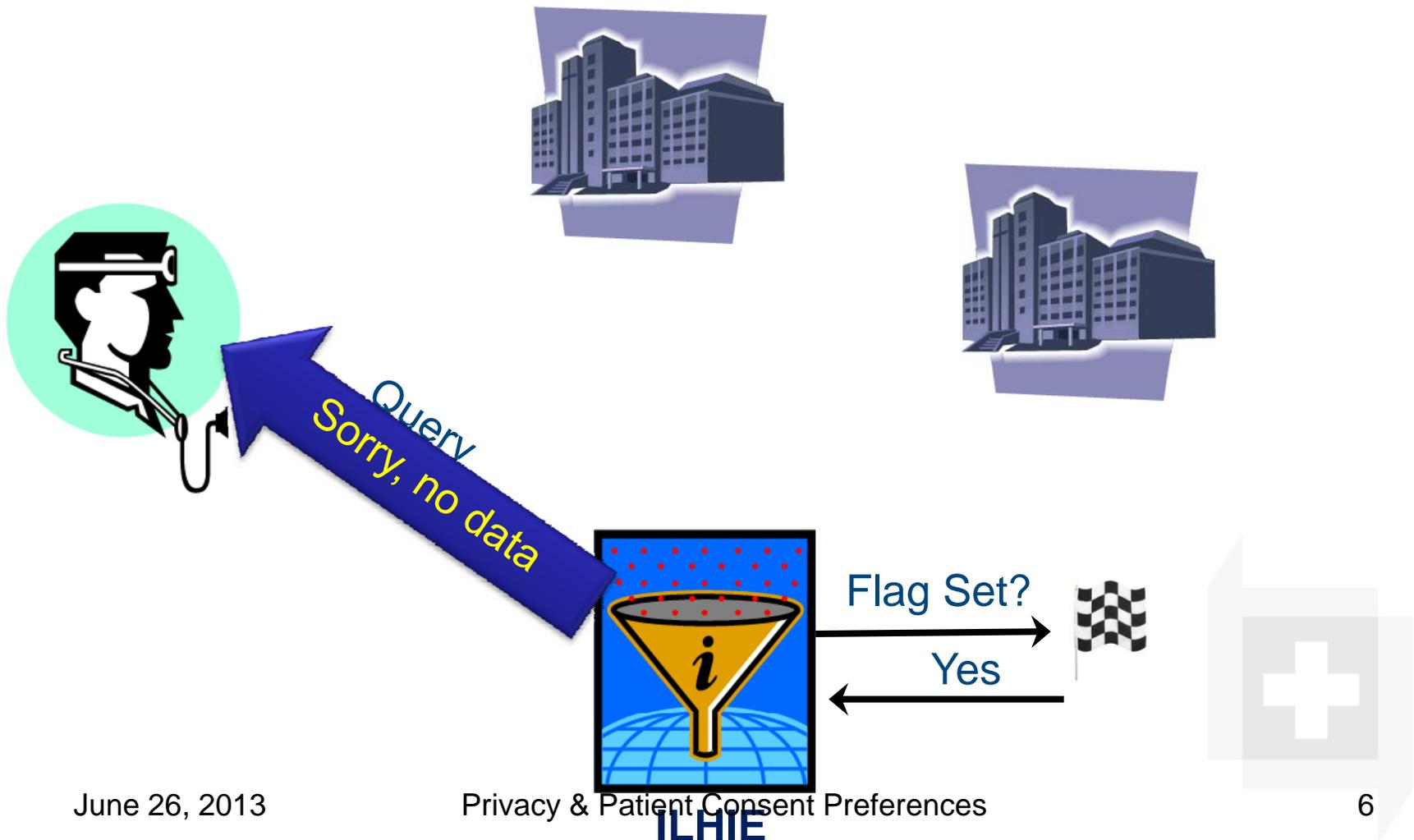
Flow of Clinical Records through ILHIE



June 26, 2013

Privacy & Patient Consent Preferences

Opt-Out flag action



- Opt-Out policy is based on all-or-nothing
 - Patient can share all her data via ILHIE or
 - Patient will share no data via ILHIE
 - Currently can't share partial records
- Provider can query/set the flag
 - From EMR via XDS.b
 - Must send an XACML message
 - Via a Web service
- ILHIE is exploring using Opt-Out flag to support EMRs that cannot handle Opt-In requirements

Granularity and Consent



- Electronic Medical Records are segmented
- C32 format has 17 sections:

Advanced Directive	Allergy / Drug Sensitivity	Comment
Condition	Encounter	Healthcare Provider
Immunization	Information Source	Language Spoken
Medication	Person Information	Plan of Care
Pregnancy	Procedure	Support
Vital Signs	Results	



- What should be the fundamental unit of consent?
 - The whole record?
 - The section?
 - Fields within sections?
- What type of tagging should be used?
 - Tags that specify sensitivity?
 - Tags that specify clinical content?
- What are the advantages and disadvantages?
- What are other approaches/considerations?

Further Sequestration Questions



- Criteria for effective sequestration/redaction?
- What is the role of patients in making sequestration decisions?
- What are patient expectations with regard to sequestration?
- How can unintended consequences be minimized or avoided?



- Data center breaches
 - Perimeter breaches
 - Unencrypted data backup
 - Insider breaches
- Devices
 - Media such as DVDs, jump drives
 - Laptops
- Transitive breaches
 - Someone steals PHI from a connected entity

- Standard perimeter security
 - Firewalls, Demilitarized zones, etc.
 - Audit trails
 - Annual Audits
- Encryption in motion
- Encryption at rest
 - HIPAA reporting not required for breach of data center
- The ILHIE is not a central repository of clinical data

- Standard Perimeter protections
 - Firewalls, Demilitarized zones, etc.
 - Audit trails
 - Annual Security audits
- Encrypt all sensitive data
 - At rest on servers
 - On backup tapes
- Encrypt all devices
 - Laptops
 - Jump drives

Ivan Handler

Ivan.handler@illinois.gov

