Day 2- Exercise 1

For technical difficulties email cryan@irishealthsolutions.com

#HcDIR2019

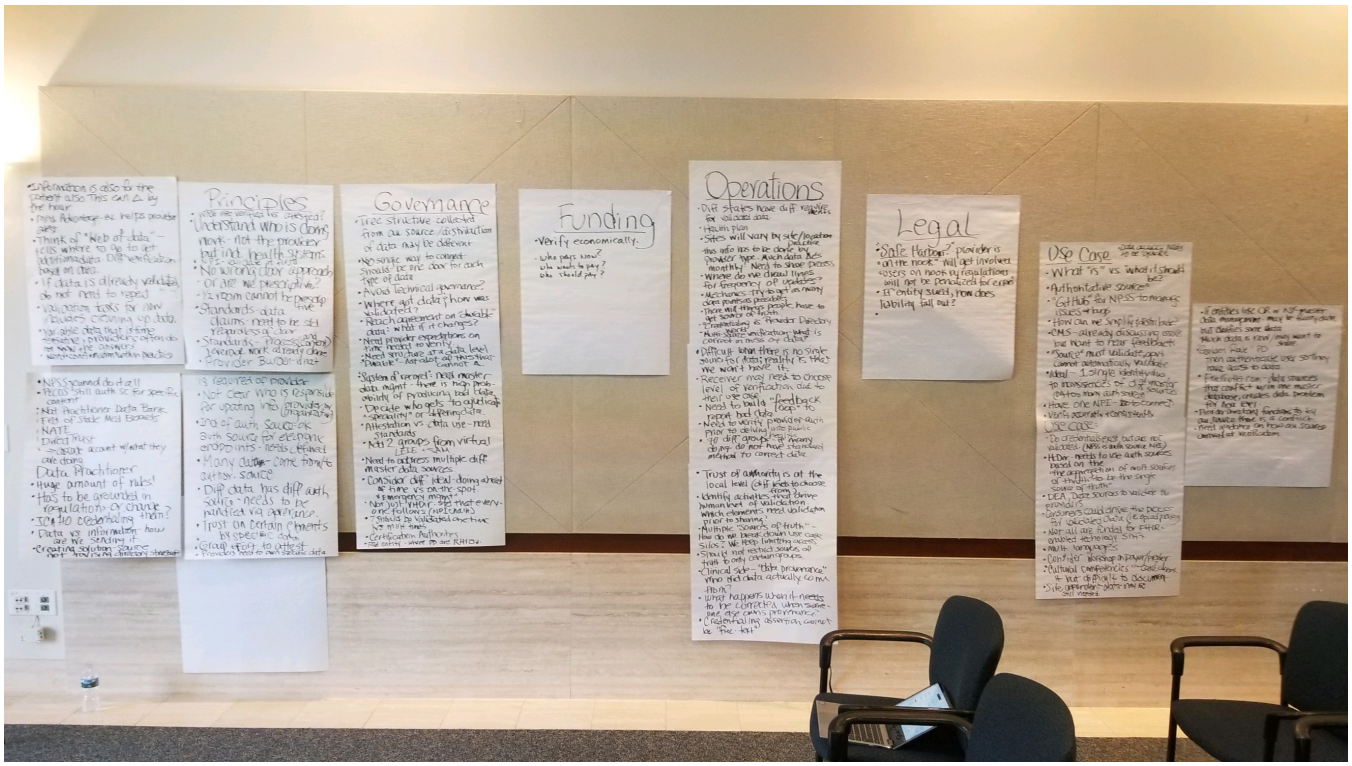
Disclaimer: The content in this space is DRAFT and will change in the next coming weeks once recordings have been listened to.

MORNING- DISCUSSION 1

Group discussion of the governance, access controls, and operations of a validated healthcare directory,

facilitated by a specific use case based on data priorities and verification discussion in Day 1 exercises.

(The boxes below will be updated in real time based on the in-room flip charts)



PRINCIPLES	GOVERNANCE	
Understanding WHO is doing the work/bot the provider but	Tree structure- collected from auth source/distribution	Verify economically
indiv. health systems.	of data may be different	Who pays now?
		Who wants to pay?
NPI- validate it first.	No single way to connect, should be one door for each	Who should pay?
	type of data	
No wrong door approach or are we being prescriptive?		
▪ 1/2 room says can't be prescriptive	Avoid technical governance?	
Standards- data claims need to be standard regardless of	Where I got it and how it was validated.	
door		
• Standards process and content leverage work already done	Reach agreement about what is "durable": what if it changes?	
Provider Burden- what is required of the provider?	Need provider expectations on time needed to verify.	
Not clear who is responsible for updating info (provider/org)	Need structure at a data level.	
Independent of authoritative source, its ok if auth. source	"Durable"- not a lot of this that "cannot" change.	
for electronic endpoints- needs to be defined.		
	System of record: need master data mgmt.- there is	
Many data come from auth. source.	high probability of producing bad data.	
Different data has different auth. source- needs to be handled	Decide who gets to adjudicate "speciality"	
via governance	or different data.	
Trust on certain elements by specific data	Attestation vs. data use need standards	
Group effort to attest	Need to address multiple different master data sources.	

Providers need to own specific data

NPESS authoritative for specific content (must account for in Cascade)

- Nat. Practitioner Data Bank
- Fed of state Med Boards
- NATE
- DirectTrust

Data Practitioner

Huge amount of rules!

Has to be grounded in regulations

JCAHO credentialing

Data vs. information- how are we sending it?

Creating a solution-source not revising directory structure.

Information is also for the patient. This can change

by the hour.

Med advantage- ex. helps provider attest.

Think of "web of data"- tells where to go to get additional data.

Diff. verification based on data.

If data is already validated, do not need to repeat

- validation/ data tracking/mgmt component.

TAXID number as well as EIDN? (Virtual attendee added)

Validation tasks for now includes cleaning up data.

Variable data that is time sensitive, providers often do not know

the answers. Need confirmation within practice.

Look at:

- List of Excluded Individuals/Entities (LEIE)
- System for Award Management (Sam.gov)

Data accuracy needs to be lightweight and quick

Consider different ideals for doing ahead of time

vs. on the spot. "emergency management".

Not just talking about stds for validating but a std that

everyone follows (NPI Chain)

Do we want to say this should be done one time and

one time only (validation)

Certification Authorities

Fed entity- where PD are RHIO

Trust of authority is at the local level (diff levels to

choose from)

Identify activities that drive human level of

verification before they happen.

- Which elements need validation prior to sharing?

Multiple "sources of truth"- How do we break down

use case silos? We keep limiting access

- Should not restrict sources of truth to only certain groups

Clinical side- "data provenance" who did data come from,

who is the source?

- what happens when data needs to be corrected
  - some one else owns it- needs to be corrected from the source?

Credentialing assertion cannot be "free" text

Use Case

What "is" vs. "what should be".

Root cause- significant bugs w/ systems with no way to express bugs back and say "this is a priority". Need a way to communicate that there are important details not being fixed.

- proposal: GitHub repository with no code which is issue tracker for NPESS

- How can we simplify & distribute?

Need an authoritative source

CMS- already discussing issues but want to hear feedback

"Source" must validate; Gov't cannot automatically validate

Ideal word "1 single directory, 1 single source of truth" due to inconsistencies of diff master data sources

- Matter of connecting indiv data sources.

Cara (Virtual attendee) need to understand how others ingest data. Not all entities are JSON/FHIR enabled or budgeted for this shift in technology.

- Proposed next steps we have a health plan payer workshop, vendor workshop and provider (defined in the regulatory mandate) workshop. This process will increase awareness, obtain additional representatives to help support the technology shift and/or our use cases allow for multiple languages like EDI 274 Provider Directory/Credentialing/Contracting TR3. Thid TR3 will be available for multiple language transaction as well as allow the user to transact with multiple entities within one single transaction so the user does not have to enter the data in mult applications or infrastructures.

Verify accurately, verify for everyone, if primary source should validate for everyone who needs to do the job and do accurately. Shouldn't have to "know someone".

Do credentials exist, but are not validated? (NPESS is auth of NPI)

HcDir- needs to use auth source based on- de-aggregation of multiple sources of truth to a single source of truth for a provider

- create golden record

DEA, Data Sources to validate the providers.

Consumers could drive the process for validated data (ie. opioid crisis)

Cultural Competencies, certain things that "we" "care about".

- site dependent data may still needed

If we have a "Golden Record" then authenticate user so that they have access to the data.

Data sources that conflict within one master database; creates data problem for next level

Need guidance on how auth source arrived at verification