S&I Data Provenance Initiative

User Stories with Record Lifecycle & Provenance Events

Gary L. Dickinson
CentriHealth Public Comments
10 August 2014

Data Provenance Chain of Trust

Authenticity, Assurance

- Data provenance ensures truth (authenticity) and trust (assurance).
- Data provenance captures (and thus embodies) the source of truth – the point of data/record origination.
- Data provenance
  - If properly captured, retained, secured, managed and conveyed from the point of origination forward
  - Ensures trust to all downstream users and for all purposes to which health information may be applied.

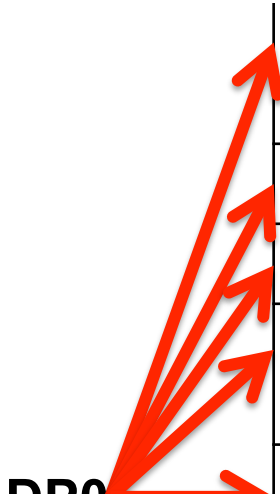
Data/Provenance PAIRS

DP0 – Source of Truth

- Point of data/record origination:
  - Is Source of Truth
  - Is Anchor for Chain of Trust
  - Instantiates a data/provenance PAIR (designated DP0)
- As it embodies the source of truth, DP0 will be considered first and always for primary use: clinical care, interventions and decision making.

Data/Provenance PAIRS

DP0 – Source of Truth



Encapsulates data and provenance as evidence of source, truth and context, including who, what, when, where and why

Is retained securely: e.g., as an EHR record entry

Is an indivisible and immutable PAIR

May be bound to the digital signature of its author and/or device/system/software of origin

Has a lifespan from point of origination to point of destruction (deletion)

Has one or more lifecycle events which occur during its lifespan, including originate/retain, also as applicable: amend, attest, access/view, exchange…
(Lifecycle events are links in the DP0 chain of trust)

May be conveyed securely via an exchange artifact (e.g., CCDA)

Source, 1 off, 2 off…

Data+Provenance PAIRS (DPn)

PAIR (data+provenance)	**DP0**	**DP1**	**DP2**	**DPn**
Is →	Source of Truth	1st order derivative	2nd order derivative	nth order derivative
Is extracted/ transformed from →		DP0	• DP1 or • DP0+DP1	DP0-DPn • Singly • In combination
Typical example: when data/record content is →	Authored, captured/ created	Transformed from source to exchange artifact format	Transformed from exchange artifact to receiver internal format	Applied to secondary uses

Source, 1 off, 2 off…

Data+Provenance PAIRS (DPn)

PAIR (data+provenance)	**DP0**	**DP1**	**DP2**	**DPn**
	→	→	→	→
Is →	Source of Truth	1st order derivative	2nd order derivative	nth order derivative
Standing	Source of Truth	Transformed from source (Transformations often introduce alterations, errors and omissions in data/record content)		
Fit for Primary Use?	**Yes**	With abundant caution	With extreme caution	No(!)
Secondary Use?	**Yes**	Yes, advisedly	Yes, advisedly	Yes, advisedly
To ensure truth (authenticity) and trust (assurance)…		And unless intended solely for secondary use: Data/record derivative content (DP1, DP2…) should always be conveyed and rendered alongside DP0 as the source of truth		

Data/Provenance PAIRS

Chain of Trust

- Lifecycle events are links in the chain of trust which ensure traceability back to the point of origination (source of truth)
  - To any downstream recipient of source data/provenance PAIR (DP0)
- In the following examples, chain of trust is shown as:

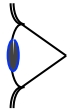
DP0 Chain of Trust – from Origination → End of Lifespan

DP1 Chain of Trust – from Translation/transformation → End of Lifespan

DP2 Chain of Trust – from Translation/transformation → End of Lifespan

DPn Chain of Trust – from Translation/transformation → End of Lifespan

Key to User Story Chain of Trust

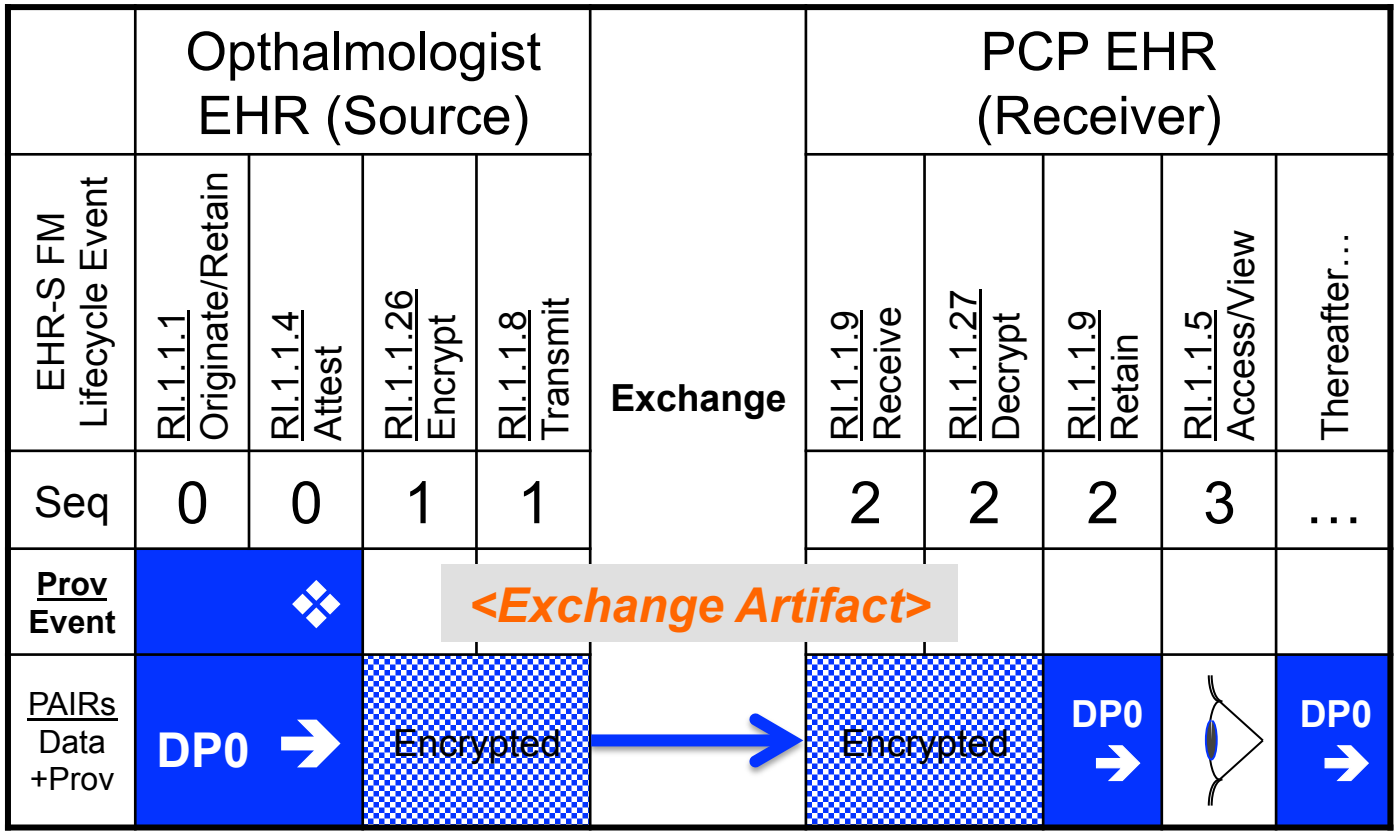
❖	= New Provenance Event
DPx	= Indivisible and Immutable Data/Provenance PAIR, instantiated at each Provenance Event
	= Ultimate Data/Record User View
RI.1.1.X	= ISO/HL7 10781 EHR System Functional Model Release 2, Record Infrastructure Section, Function Reference

User Stories

- **Scenario 1: Data Source → End Point**
- User Story 1: A patient arrives at the ophthalmologist's office for her annual eye exam. The ophthalmologist conducts an eye exam and captures all of the data from that visit in his EHR. The ophthalmologist electronically sends the information back to the patient's PCP (where all data in the report sent was created by the ophthalmologist).

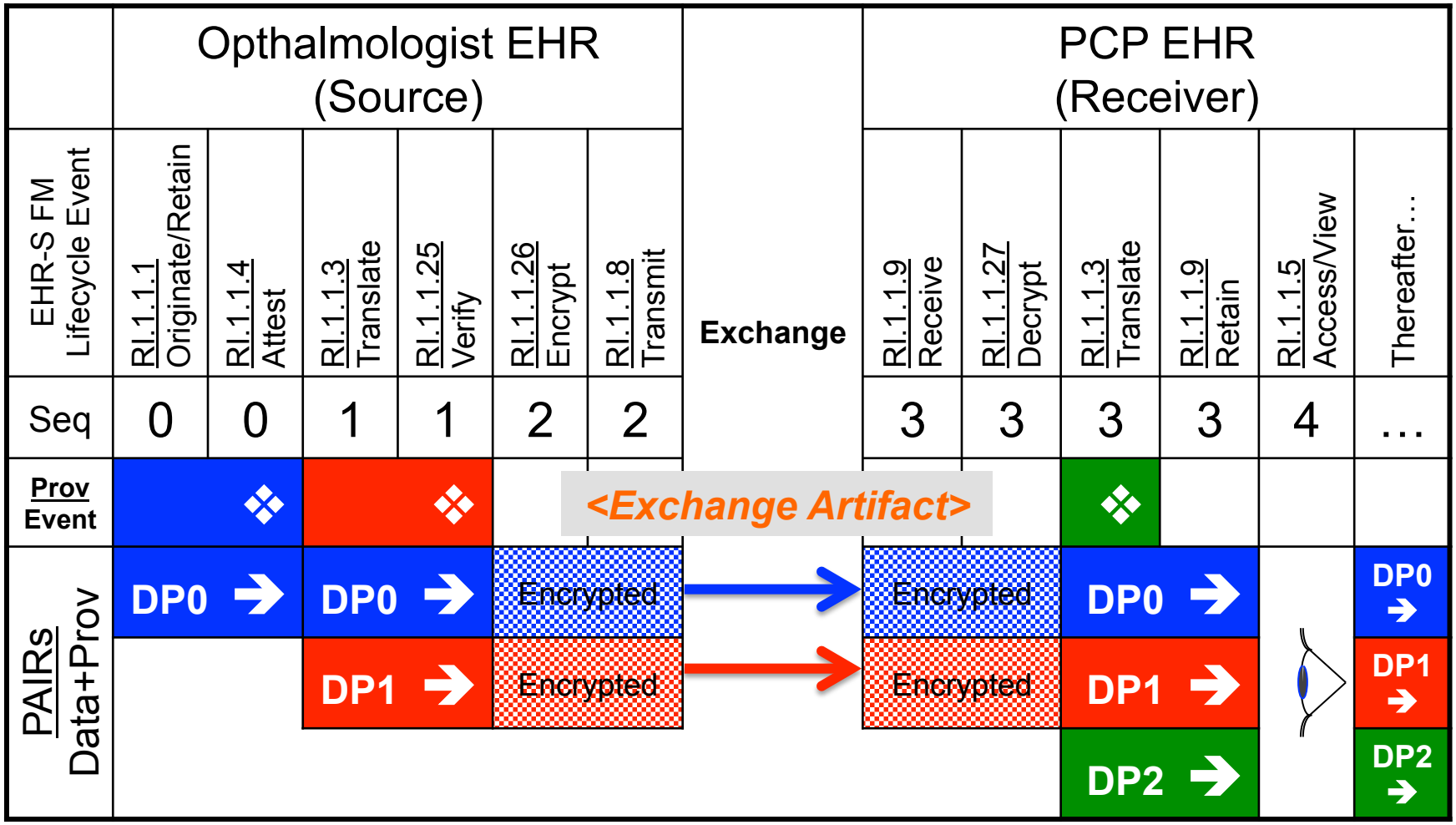
Data Provenance – Scenario 1, User Story 1

Single Provenance Event



Data Provenance – Scenario 1, User Story 1

Multiple Provenance Events

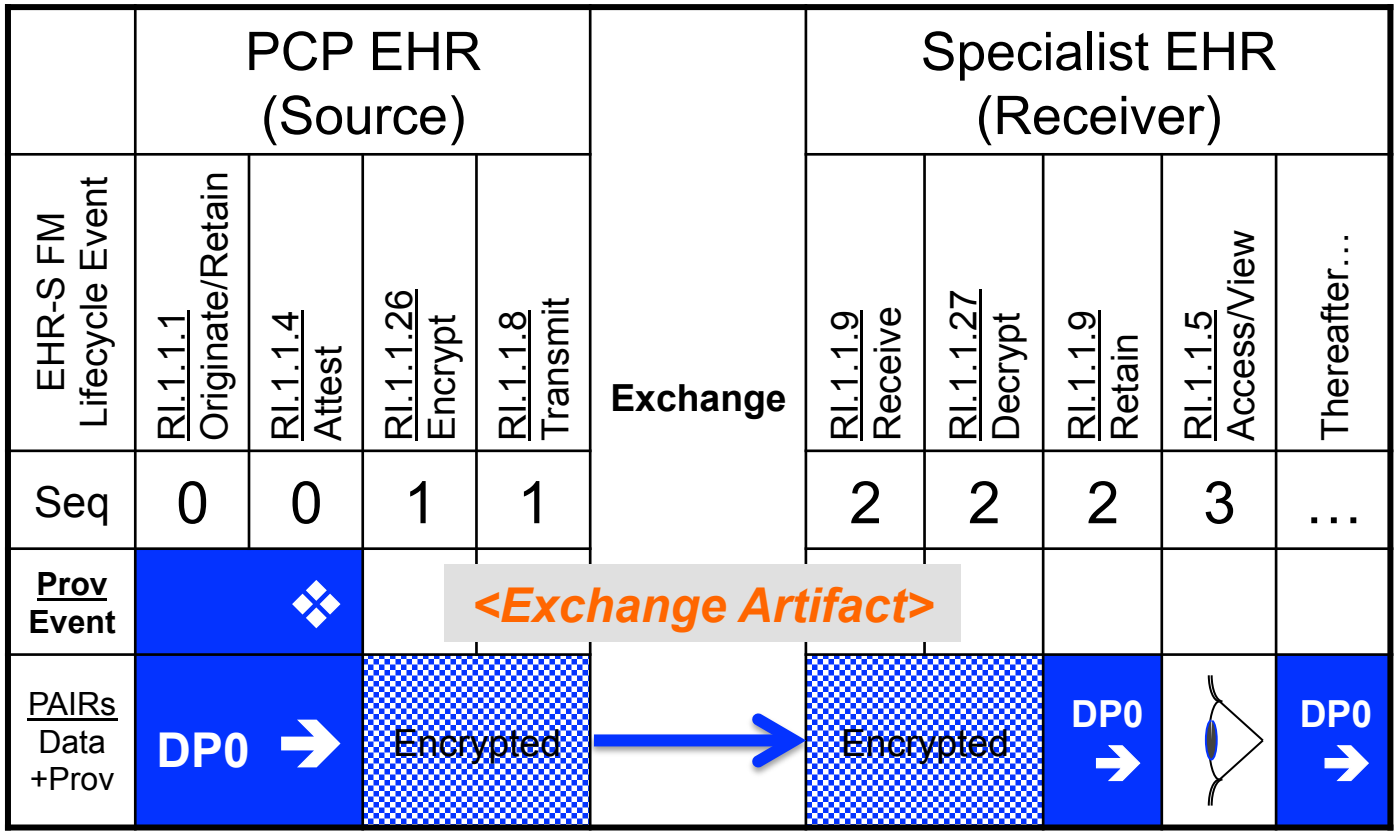


User Stories

- **Scenario 1: Data Source → End Point**
- User Story 2: A patient wishes to transmit the Summary of Care Document she downloaded from her PCP to her Specialist. Rather than downloading and sending it herself, she requests that the PCP transmits a copy of the document on her behalf to her Specialist. PCP is the only author of the Summary of Care Document and also the sender of the information to the Specialist. The Specialist understands from the document's provenance that it is authentic, reliable, and trustworthy.

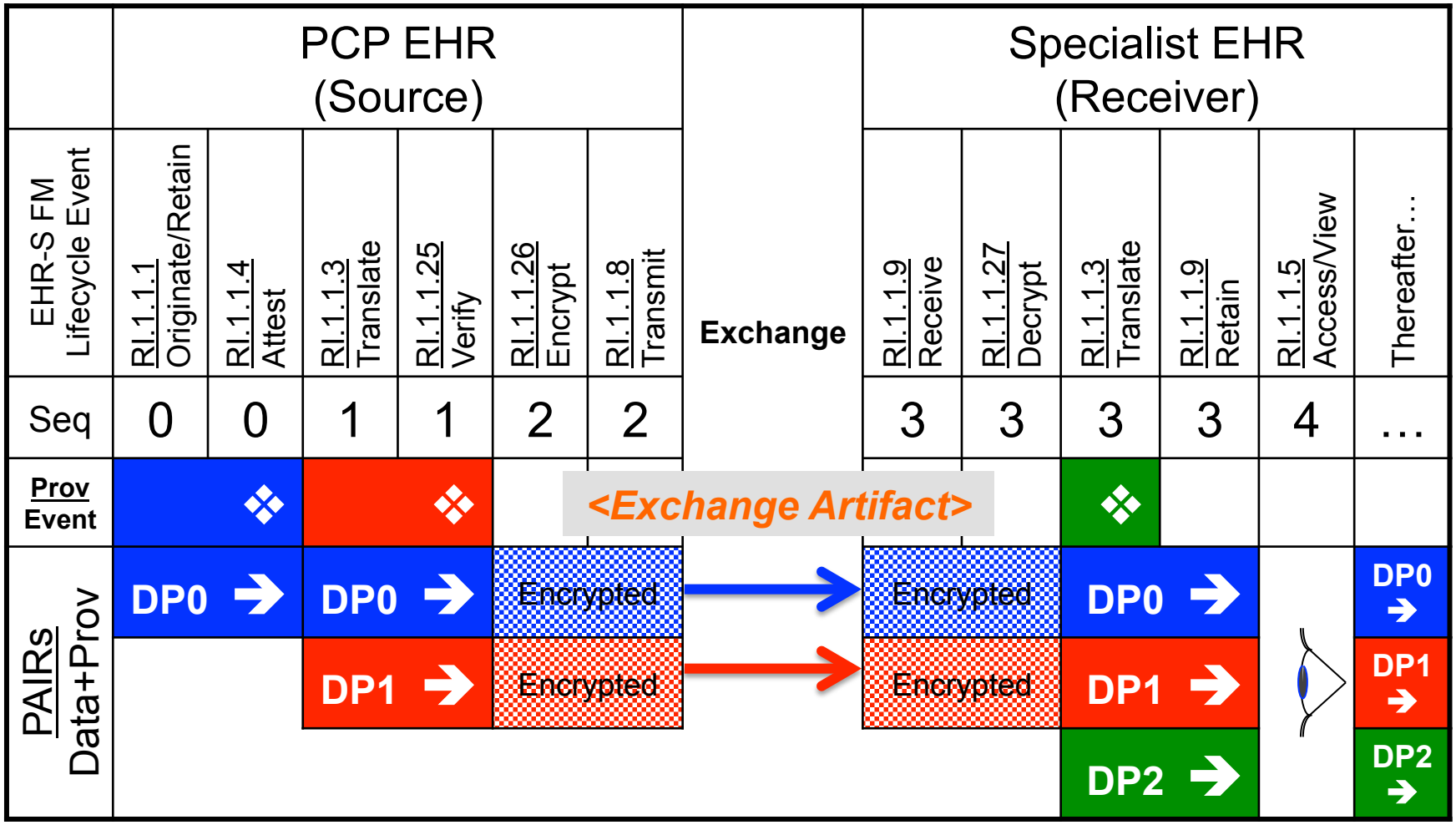
Data Provenance – Scenario 1, User Story 2

Single Provenance Event



Data Provenance – Scenario 1, User Story 2

Multiple Provenance Events

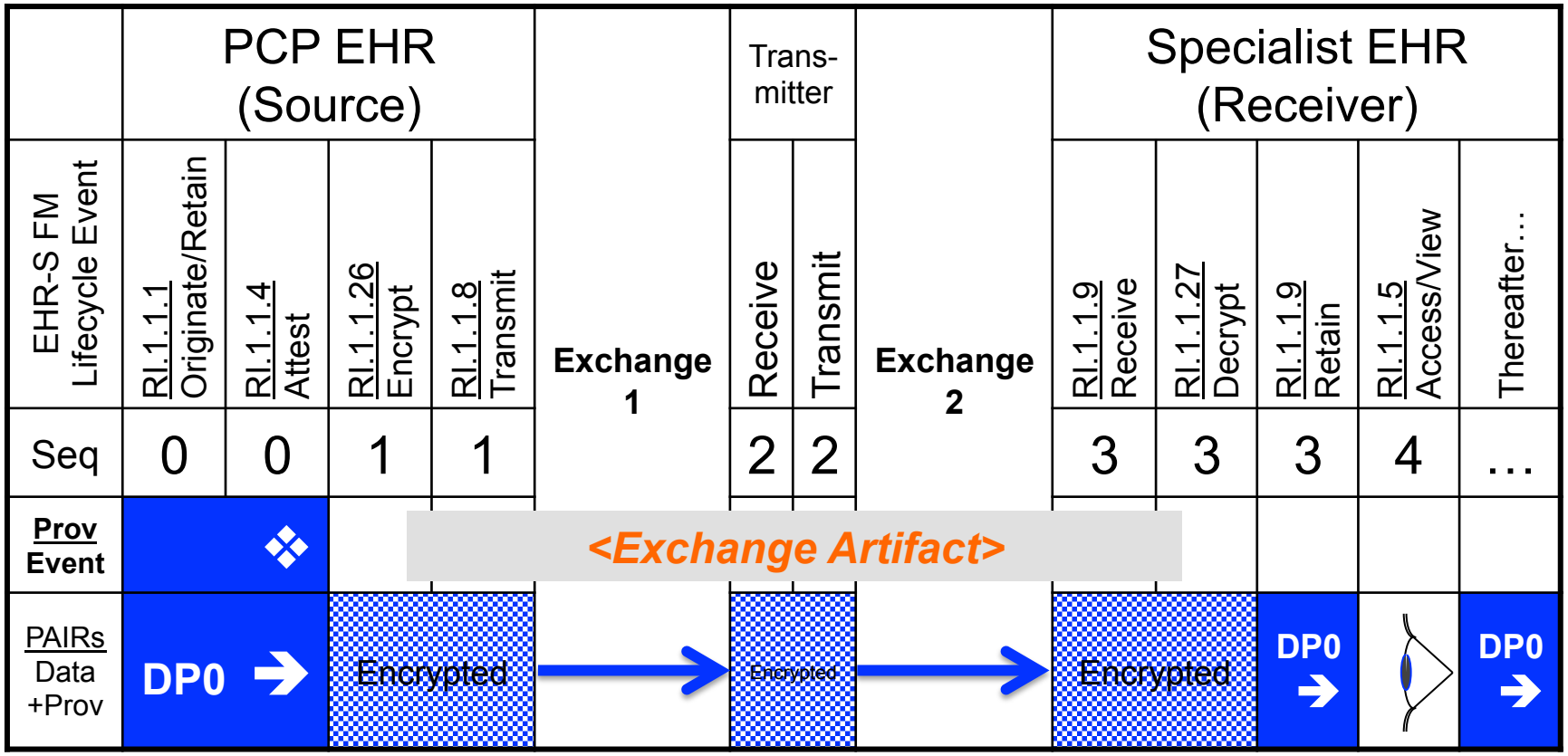


User Stories

- **Scenario 2: Data Source → Transmitter → End Point**
- User Story 1 (no alteration in exchange): While training for a marathon, a patient fractures his foot. The patient's PCP conducts a foot exam and captures all of the data from that visit in his EHR. The PCP also calls in a referral for the patient to an orthopedic specialist for further treatment. After the PCP calls in the referral, the summary of care information is made available to the specialist, by passing through a transmitter, before being received by the orthopedic specialist's system. The orthopedic specialist receives the summary of care with provenance information and an indication that the data passed through a transmitter.

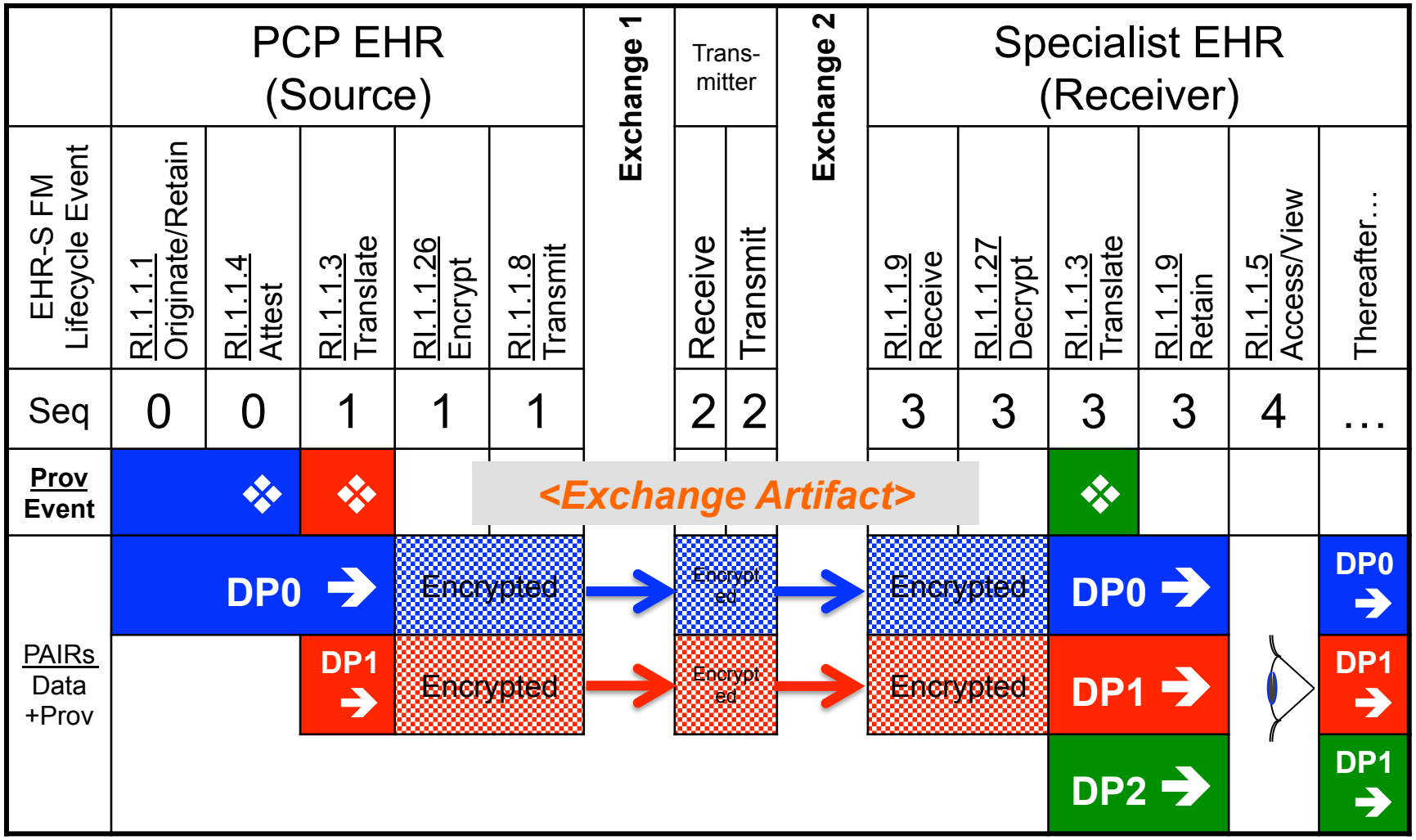
Data Provenance – Scenario 2, User Story 1

Single Provenance Event



Data Provenance – Scenario 2, User Story 1

Multiple Provenance Events

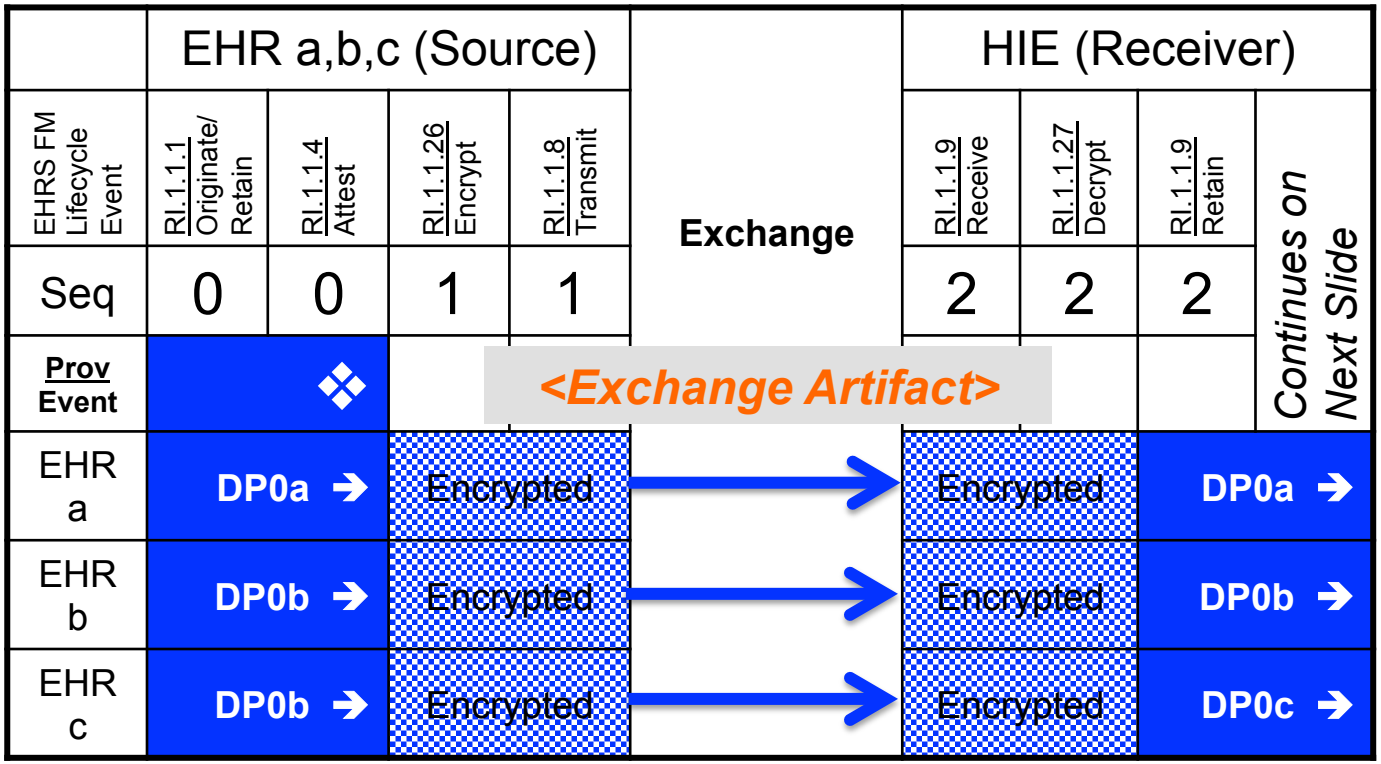


User Stories

- **Scenario 3: Data Source → Assembler → End Point**
- User Story 1: A patient is rushed to the Emergency Department due to a car accident. The physician wants to obtain the patient's summary record as part of the delivery of care. The physician queries the HIE repository and receives a summary record from the past six months. The data received includes the provenance information from the originating sources and also information that identifies the assembler and the actions they have taken.

Data Provenance – Scenario 3, PRE User Story 1

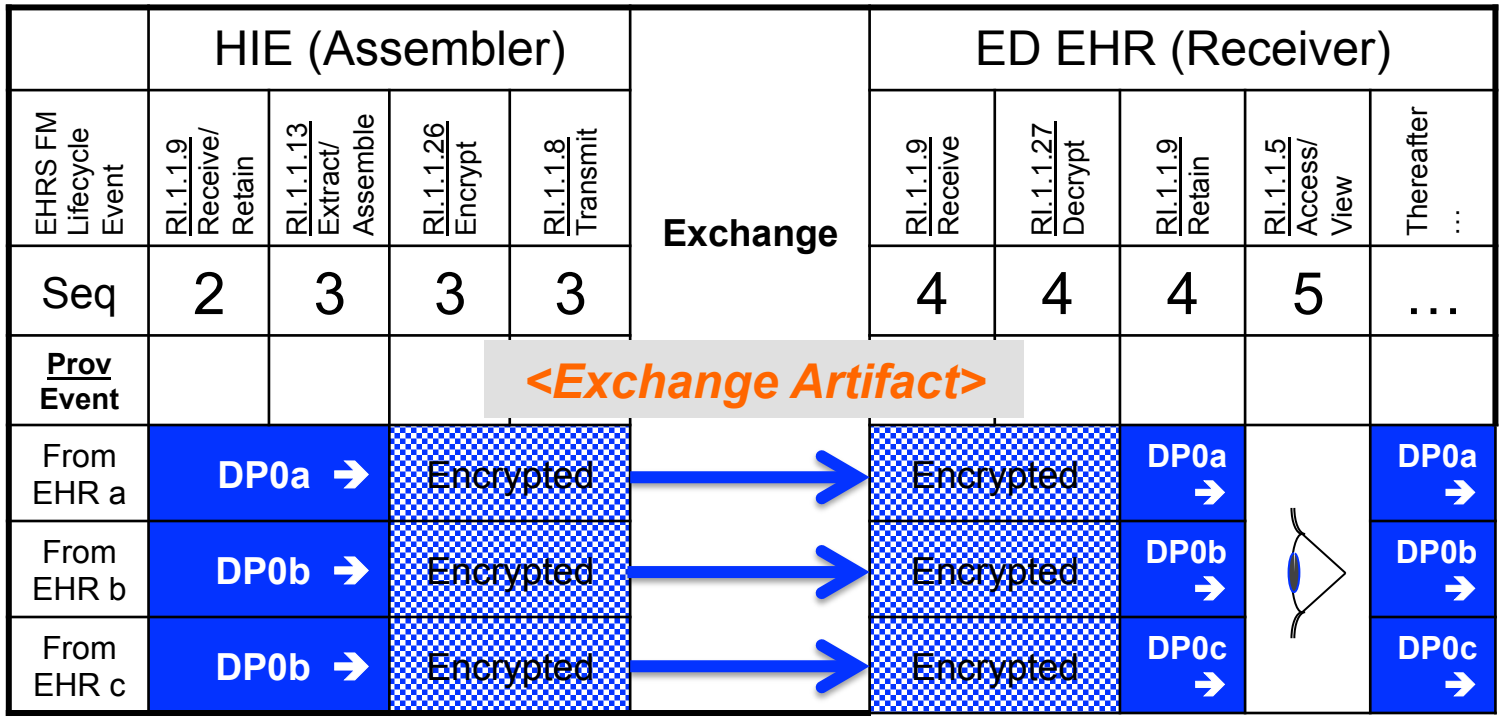
Single Provenance Event



Data Provenance – Scenario 3, User Story 1, con't

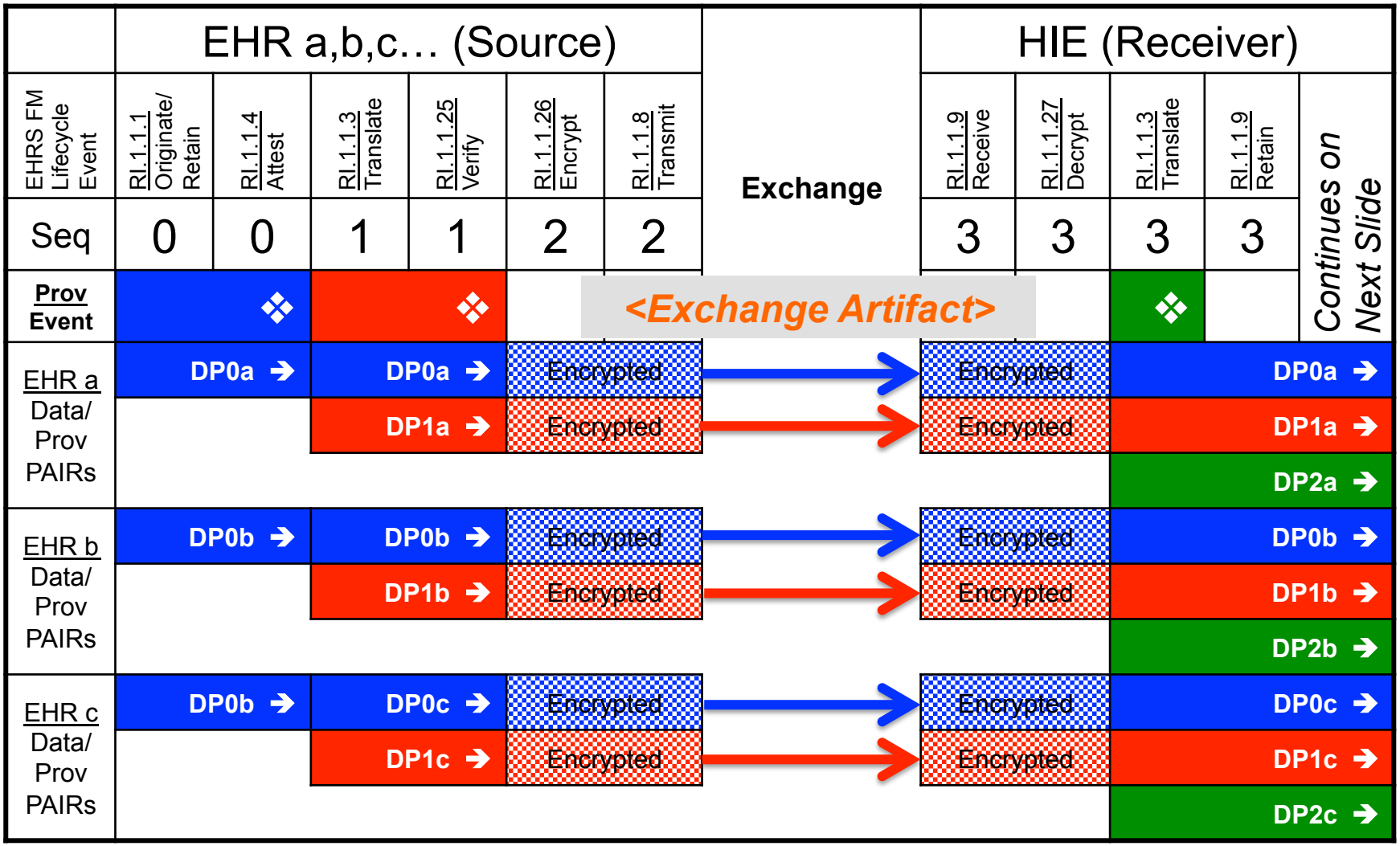
Single Provenance Event

Starting from Step 2…

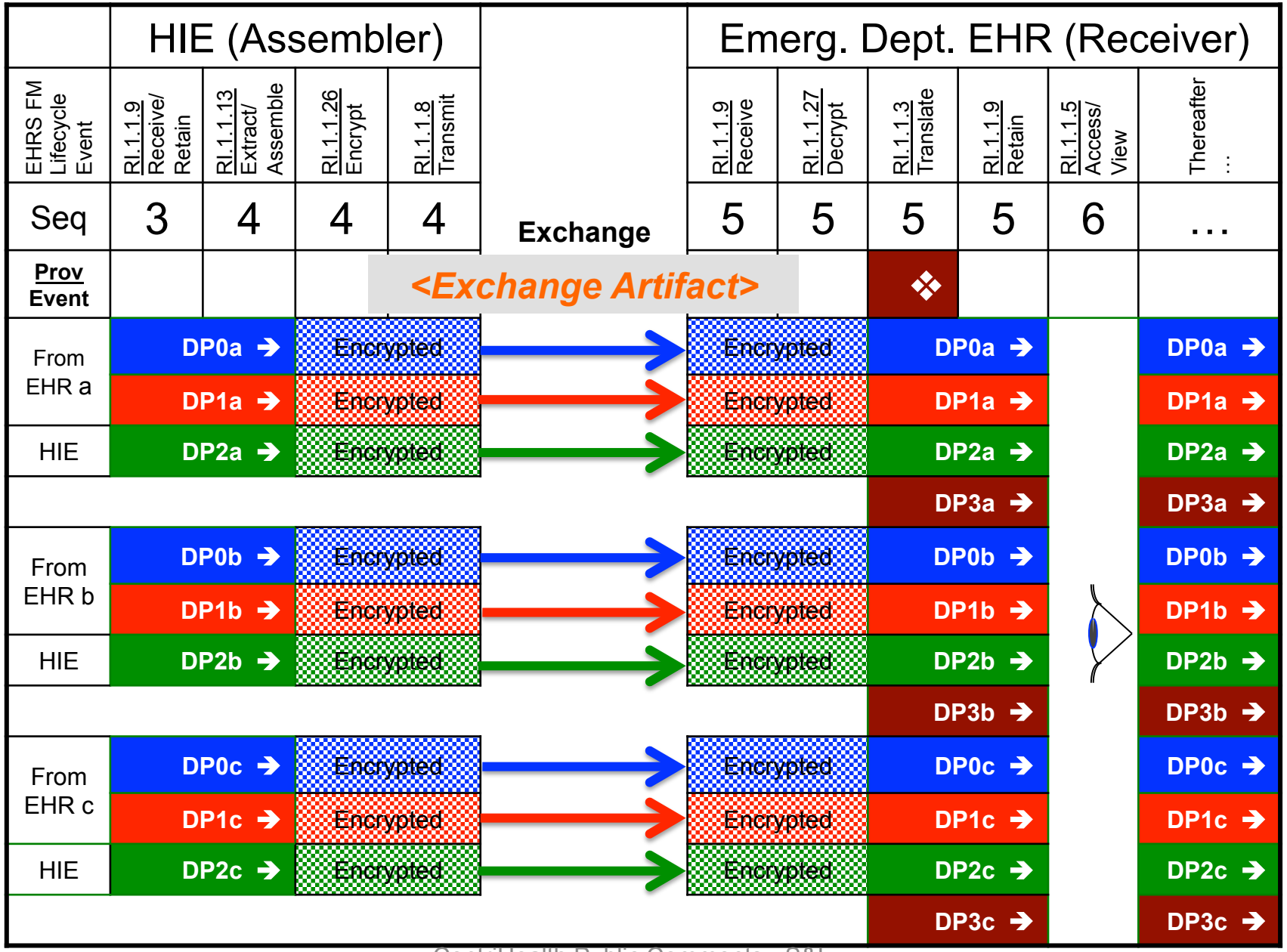


Data Provenance – Scenario 3, PRE User Story 1

Multiple Provenance Events



Starting from Step 3…

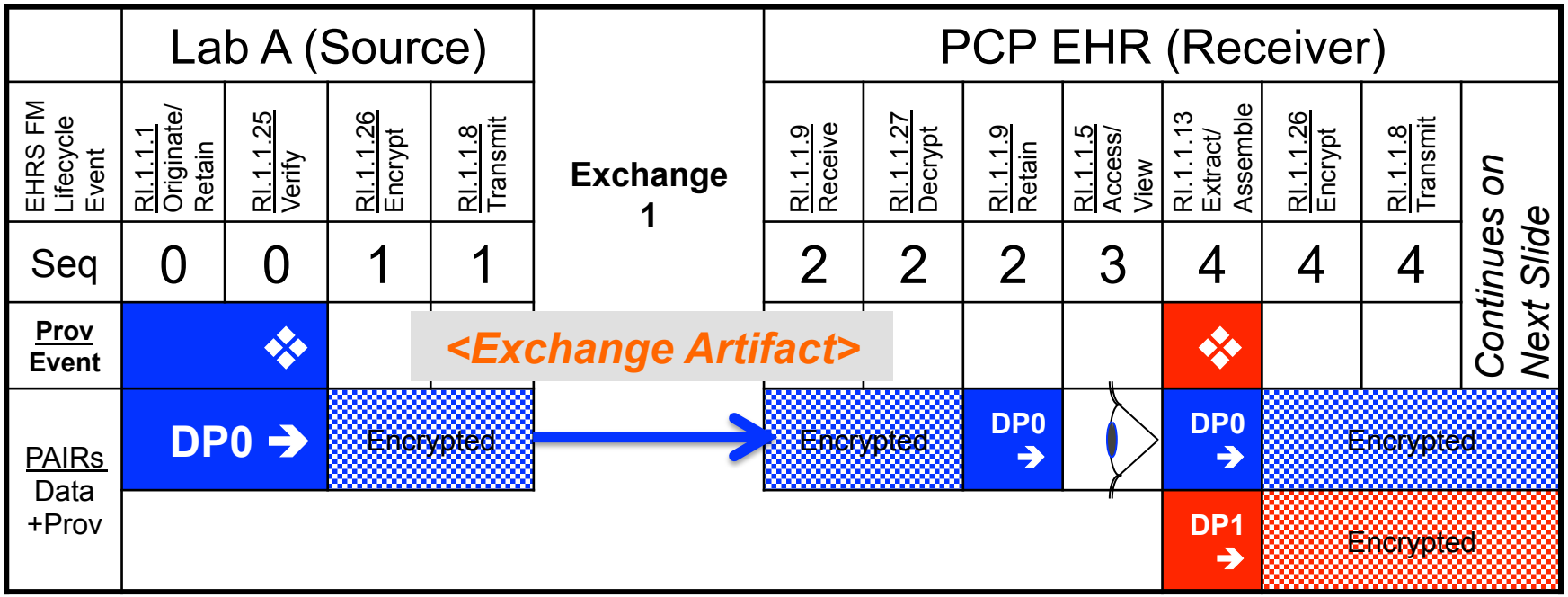


User Stories

- **Scenario 3: Data Source → Assembler → End Point**
- User Story 2: A patient with diabetes goes to Lab A to have his blood drawn. Lab A sends the lab results in a standard lab format to the PCP's EHR with provenance information attached. Upon reviewing the lab results, the PCP decides to refer the diabetic patient to a specialist for consultation. The PCP electronically sends a referral to the specialist. The referral document includes relevant data originating in the PCP's EHR along with provenance information from Lab A that is transformed into a representation that is compatible with the referral document.

Data Provenance – Scenario 3, User Story 2

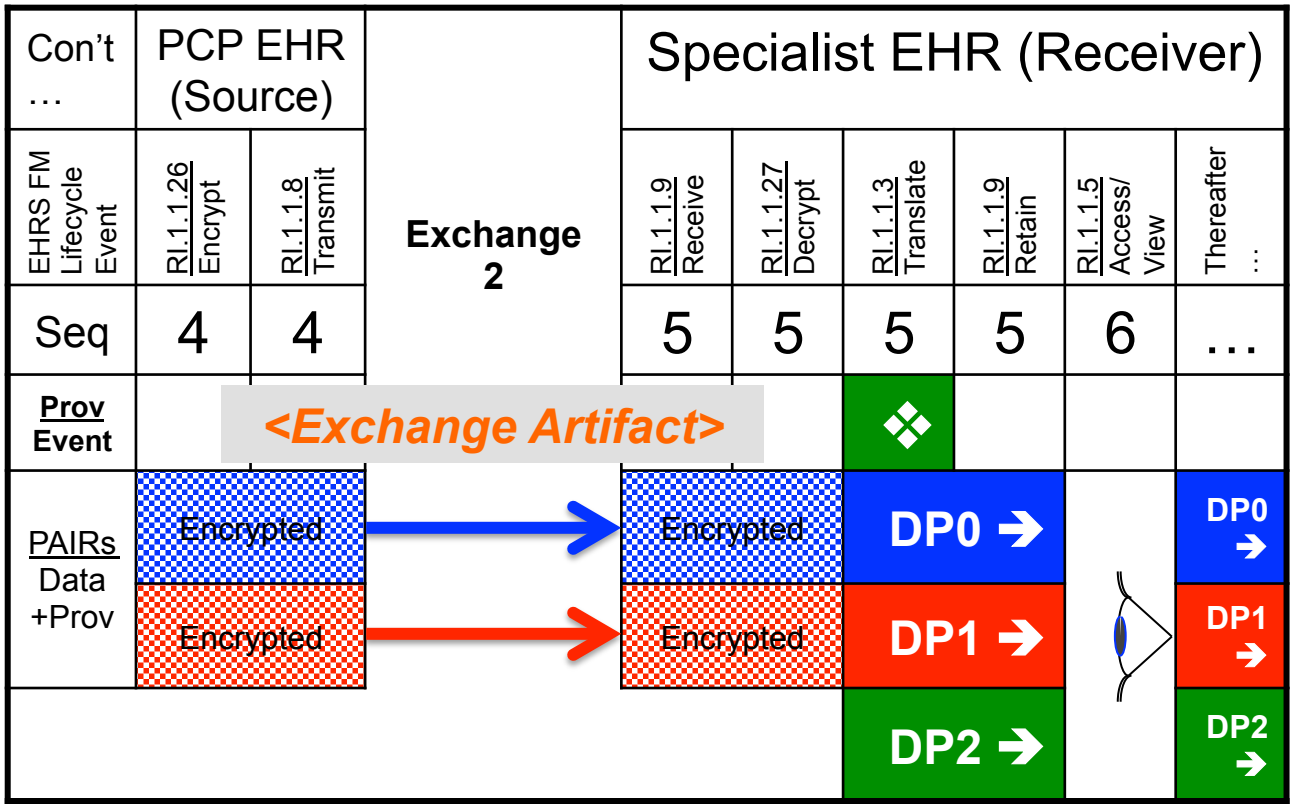
Multiple Provenance Events



Data Provenance – Scenario 3, User Story 2, con't

Multiple Provenance Events

Continuing at Step 4…



User Stories

- **Scenario 3: Data Source → Assembler → End Point**
- User Story 3: A PCP tethered PHR enables patient to download and transmit Summary of Care records that includes provenance information to anyone she chooses. Patient downloads full Summary of Care Document, disaggregates the medications, problems, and vital signs in the document and then copies these into her PHR along with medications, problems and vital signs added previously. Patient then sends selected medications, vitals, and problems from PHR to her Fitness Trainer App in a mobile device friendly format using different terminology for expressing vital sign measures. The patient authorizes the Fitness Trainer App to access the patient's information and put into a format that is recognizable by the Fitness Trainer App client. The Fitness Trainer App user (could be patient, physical therapist, etc.) receives provenance information showing that the information received has been assembled by the patient and that it was authored by various other clinical staff.

Data Provenance – Scenario 2, User Story 1

Multiple Provenance Events