StrongKey®
Securing the Core

Securing Data Across the Enterprise using SOA

Section IV
EKMI Use-Case

OASIS Open Standards
April 28, 2008

Arshad Noor, StrongAuth, Inc.
arshad.noor@strongauth.com

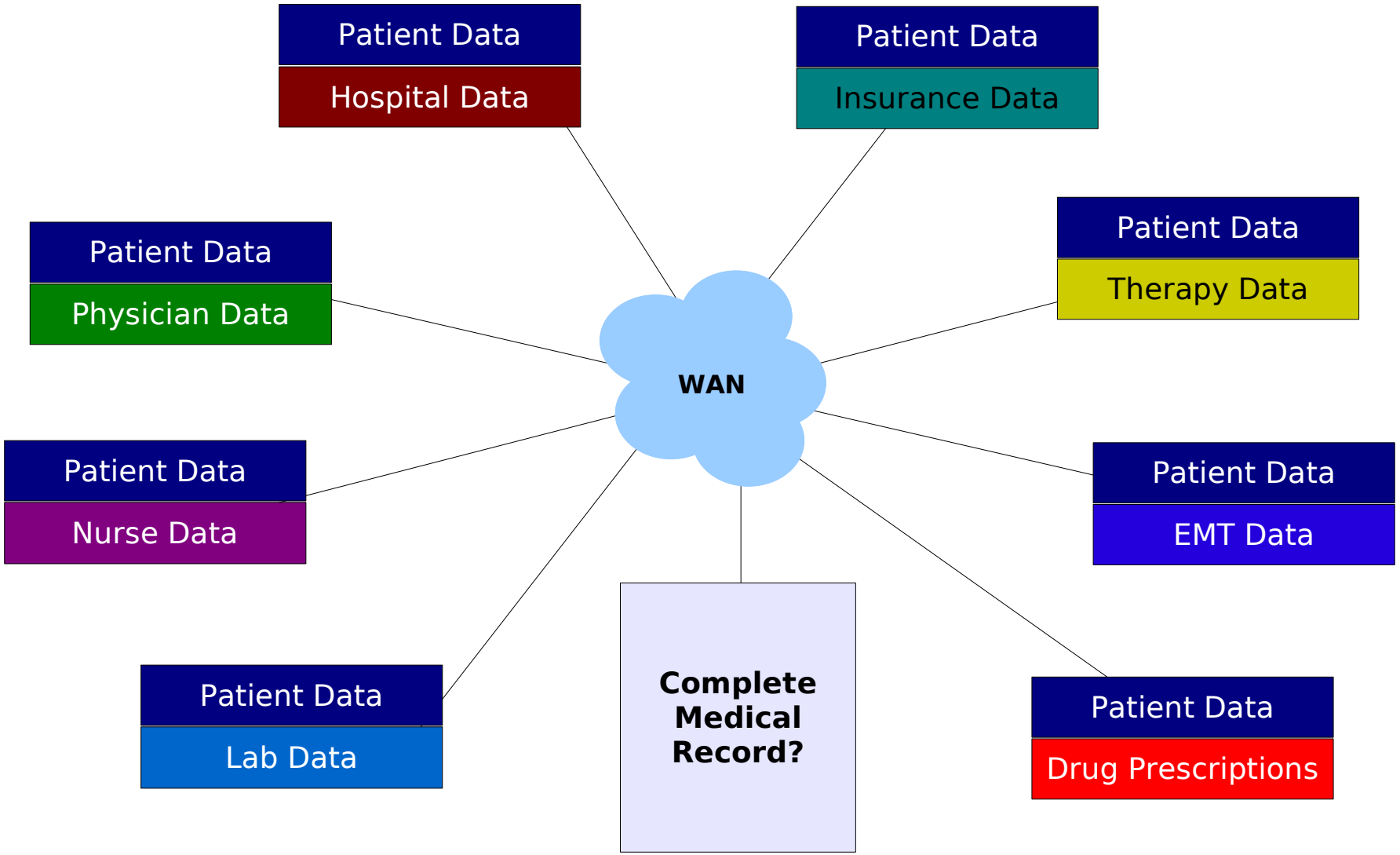
Goals

- Industry
  - Health-care
- Application
  - Electronic Health Records (EHR)
- Security goal
  - Ensure that authorized entities can access information when they need to
- Privacy goal
  - Ensure that creators/owners of information have control over sensitive information

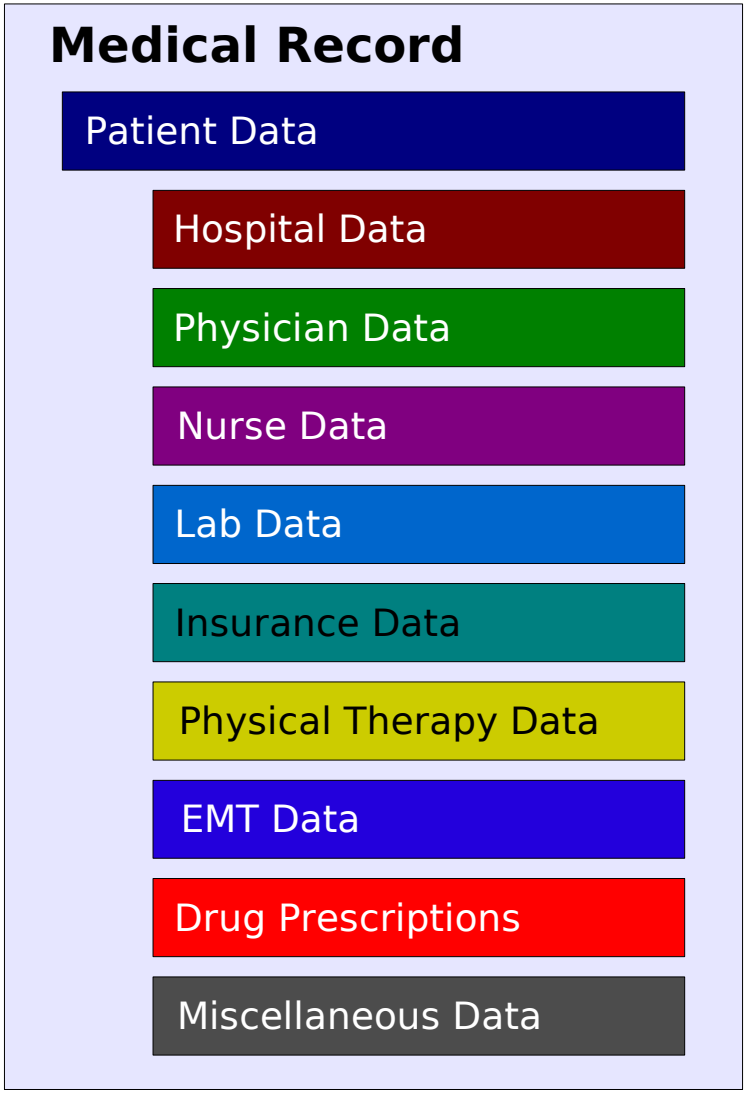
EHR Players

- Patient (PAT)
- Physician (PHY)
- Nurse (NUR)
- Emergency Medical Technician (EMT)
- Hospital (HOS)
- Diagnostic Laboratory (LAB)
- Pharmacy (PHA)
- Insurance Company (INS)
- Center for Disease Control (CDC)
- Clinical Research Organization (CRO)
- Government Agency (HHS)

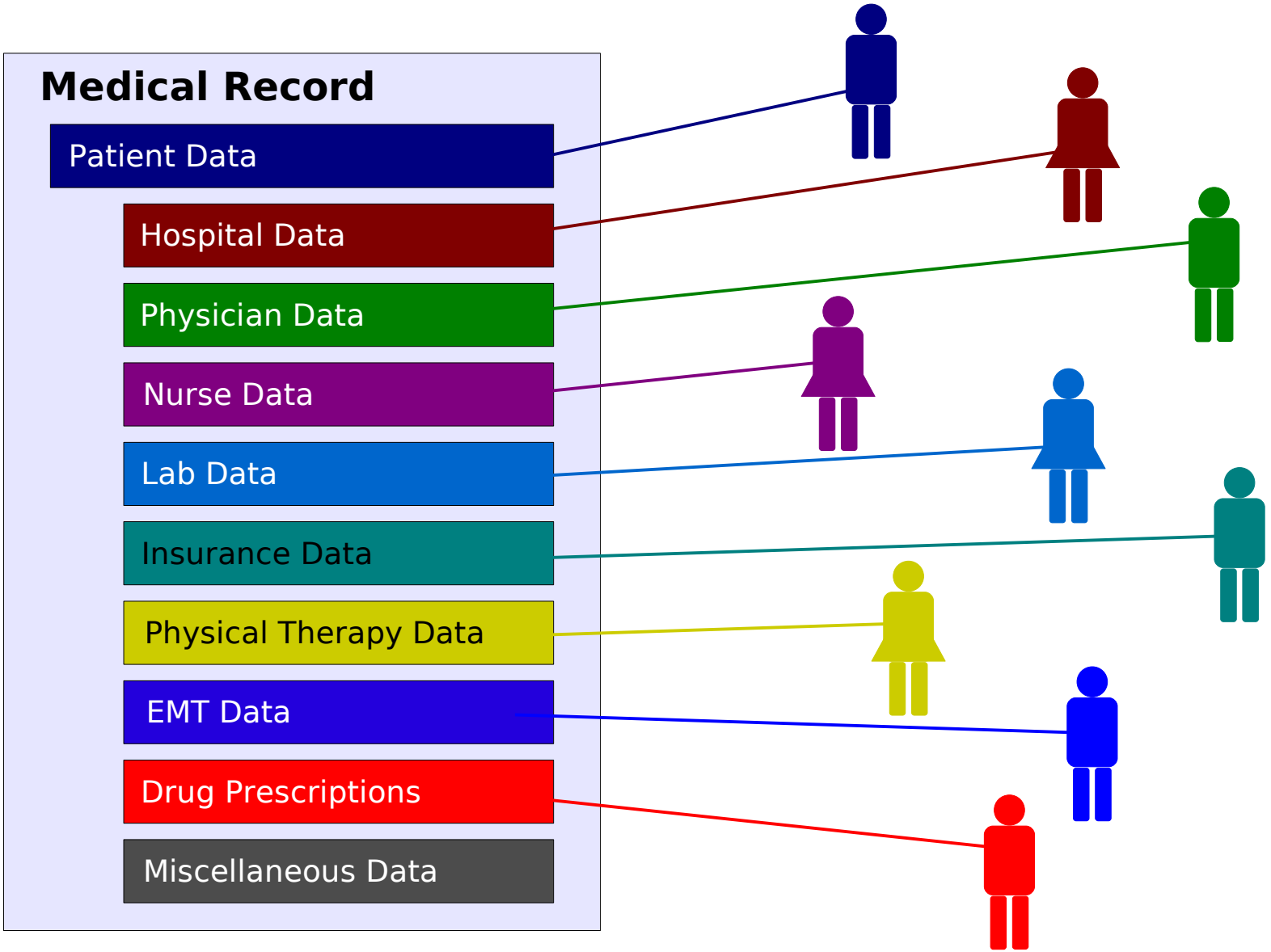
One of the Problems



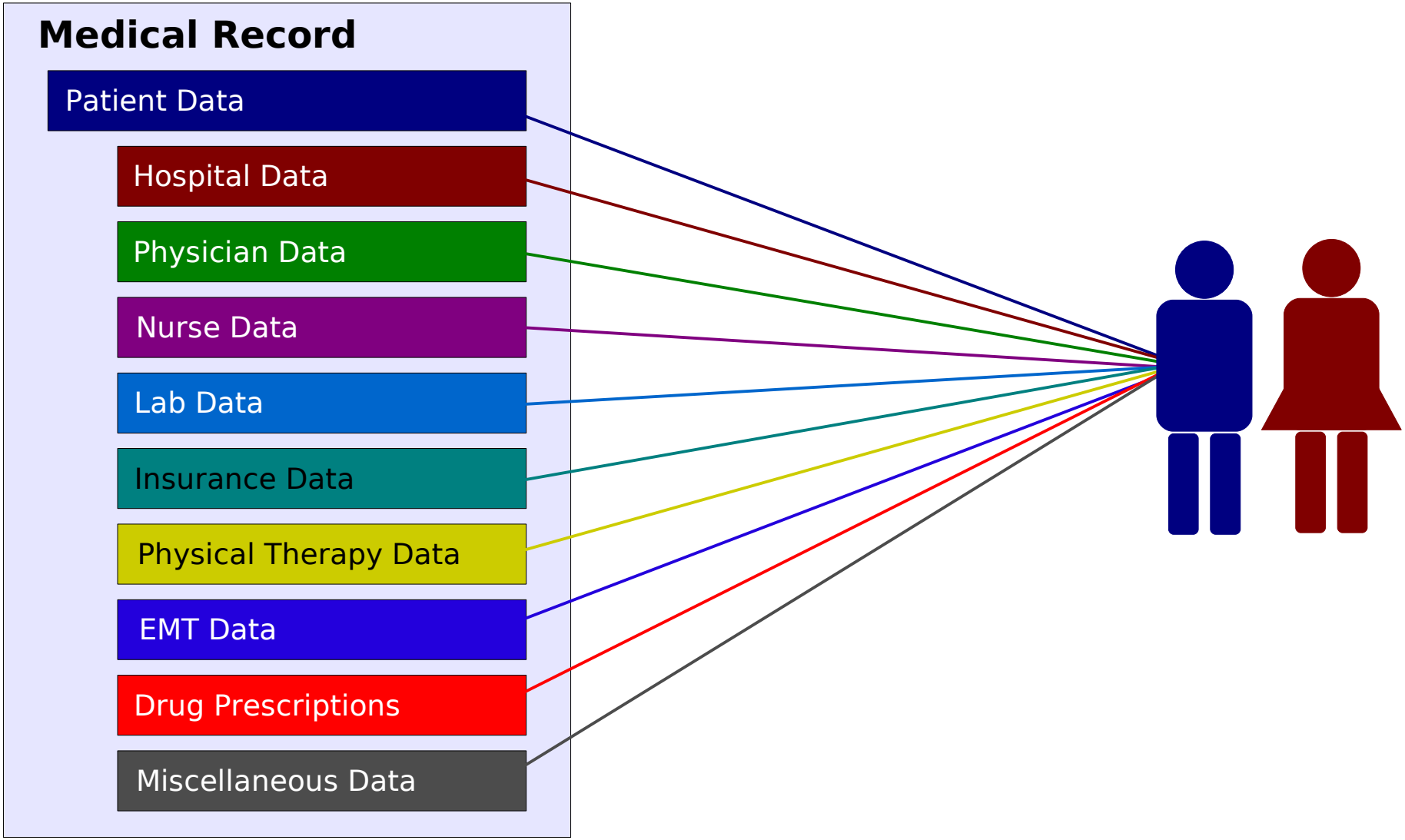
Hopefully..



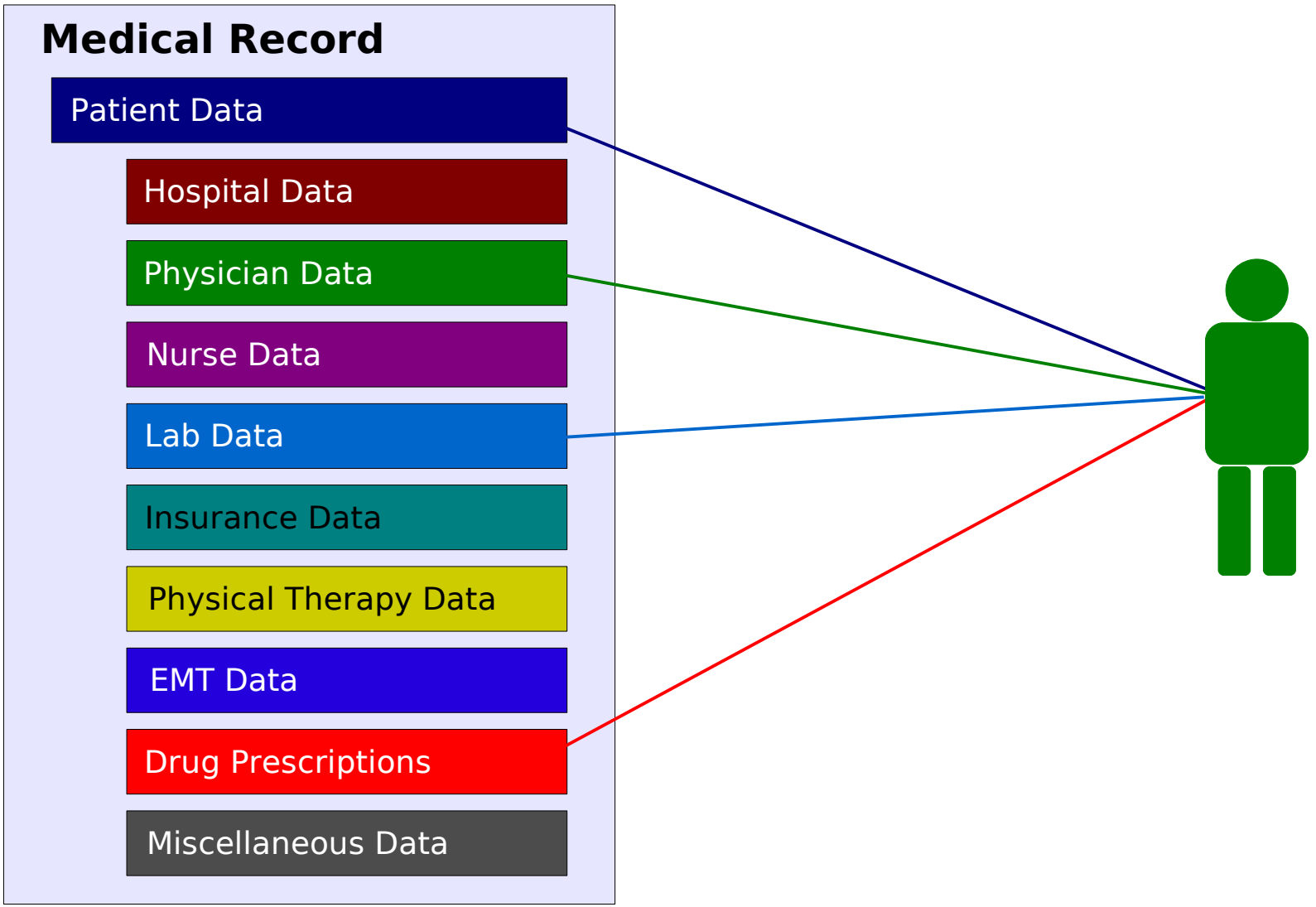
Ideally..



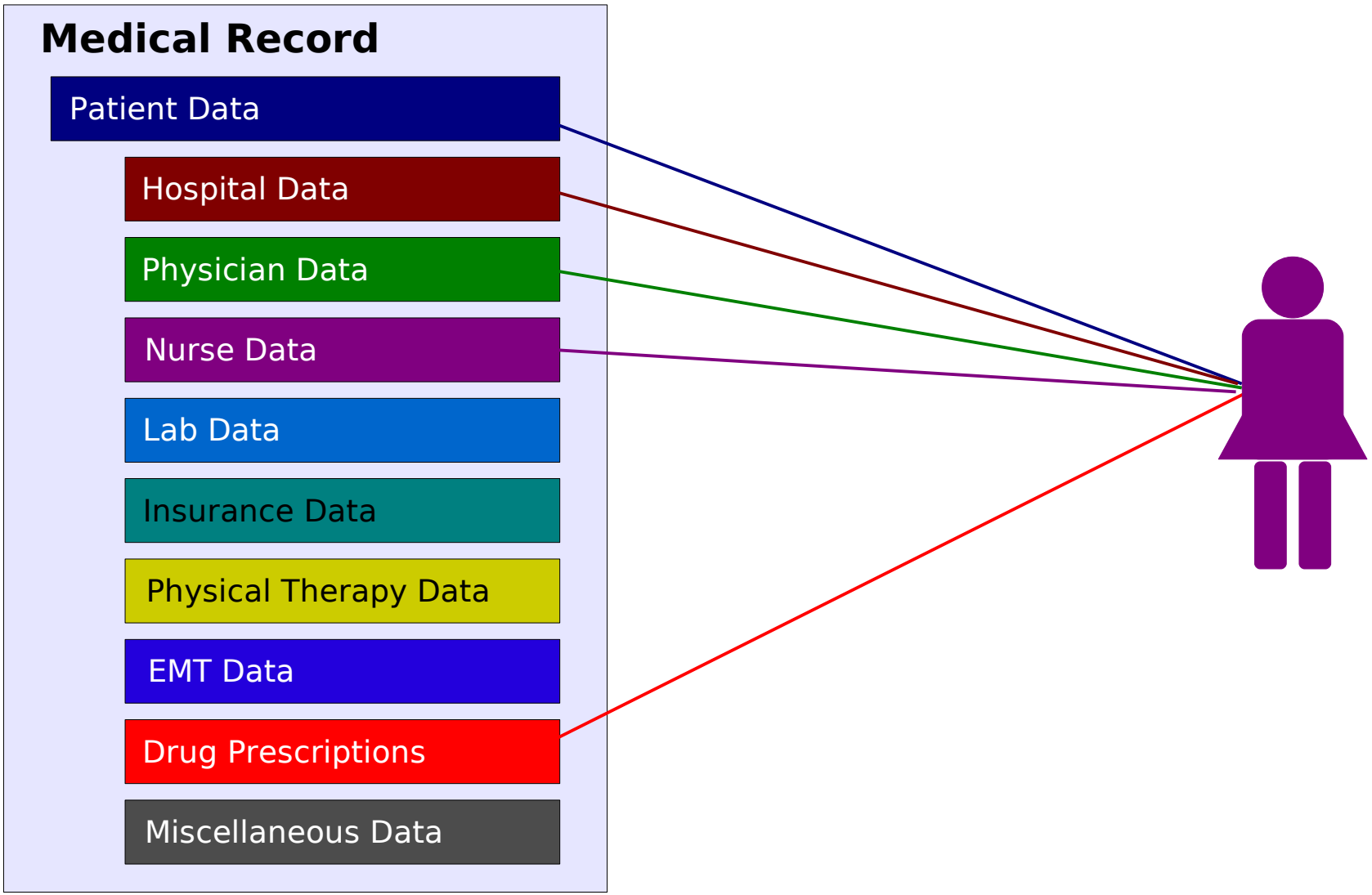
The Reality



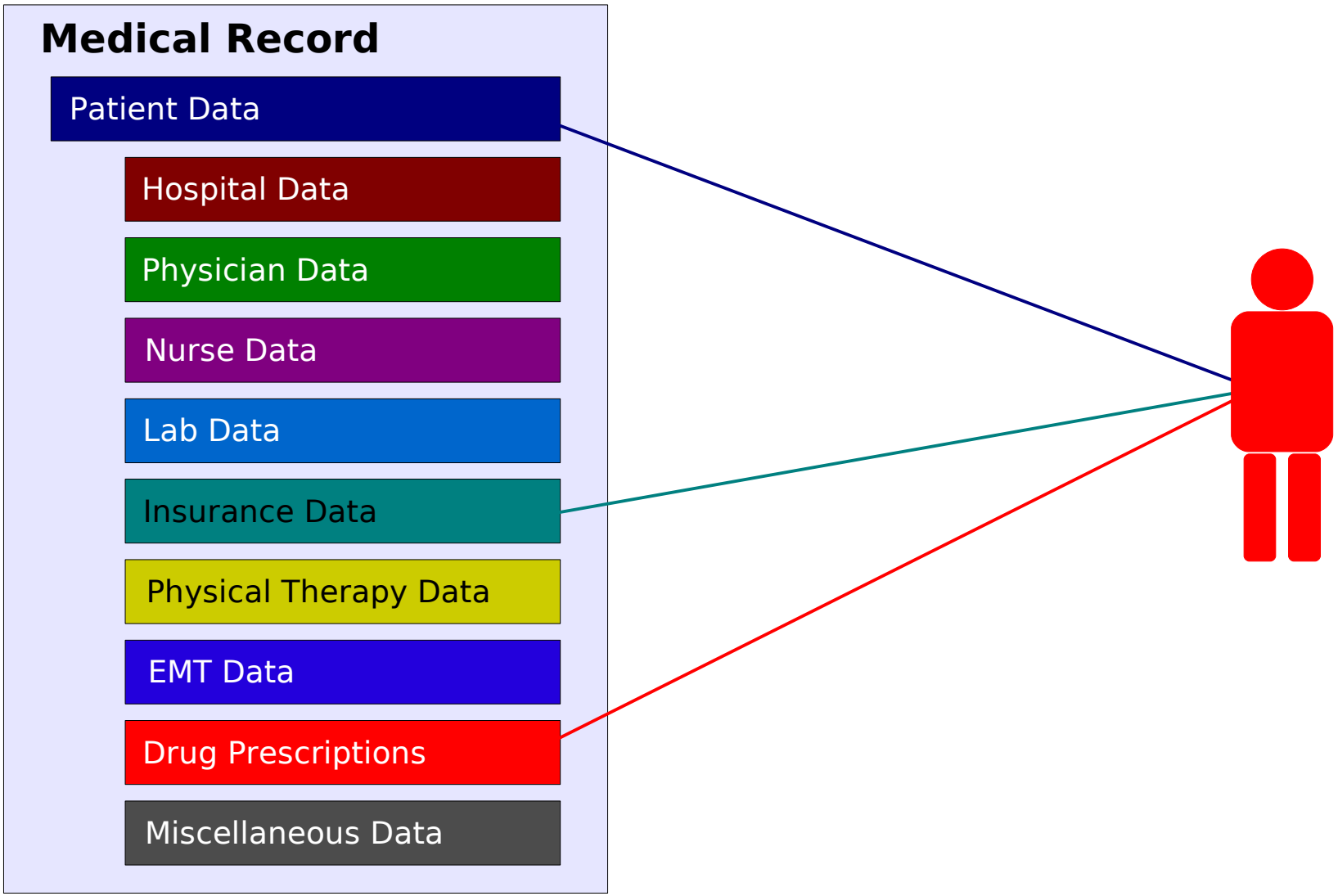
Personal Physician



Hospital Nurse



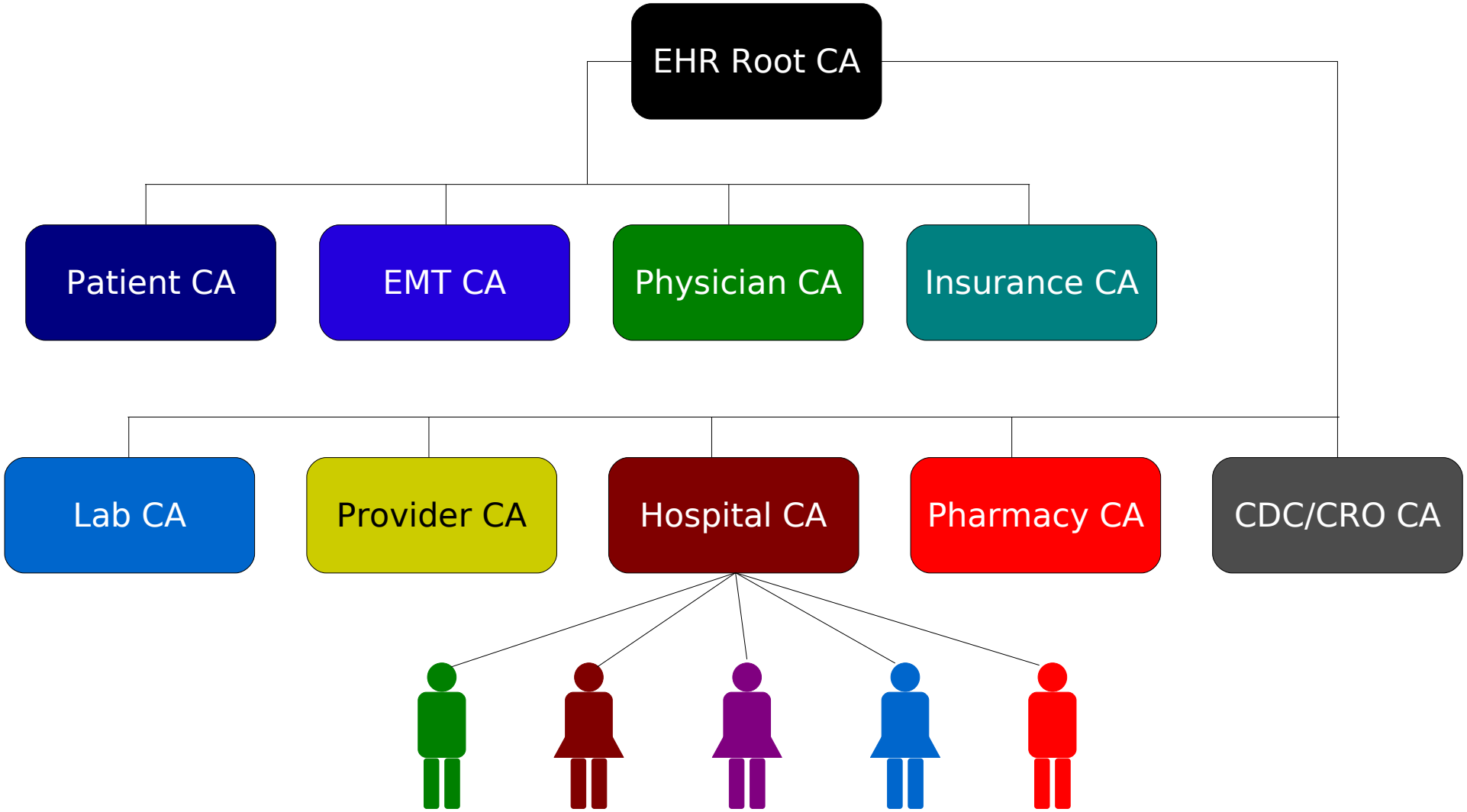
The Pharmacy



Solution Requirements

- Healthcare Industry PKI
  - Root CA managed by Federal Agency
  - Subordinate CA's for each class of entity
- XML data-model using XML Encryption
- Classification of data based on need for access
- Key-classes with 1:1 mapping with data-classes
- Applications that use this security model

EHR PKI



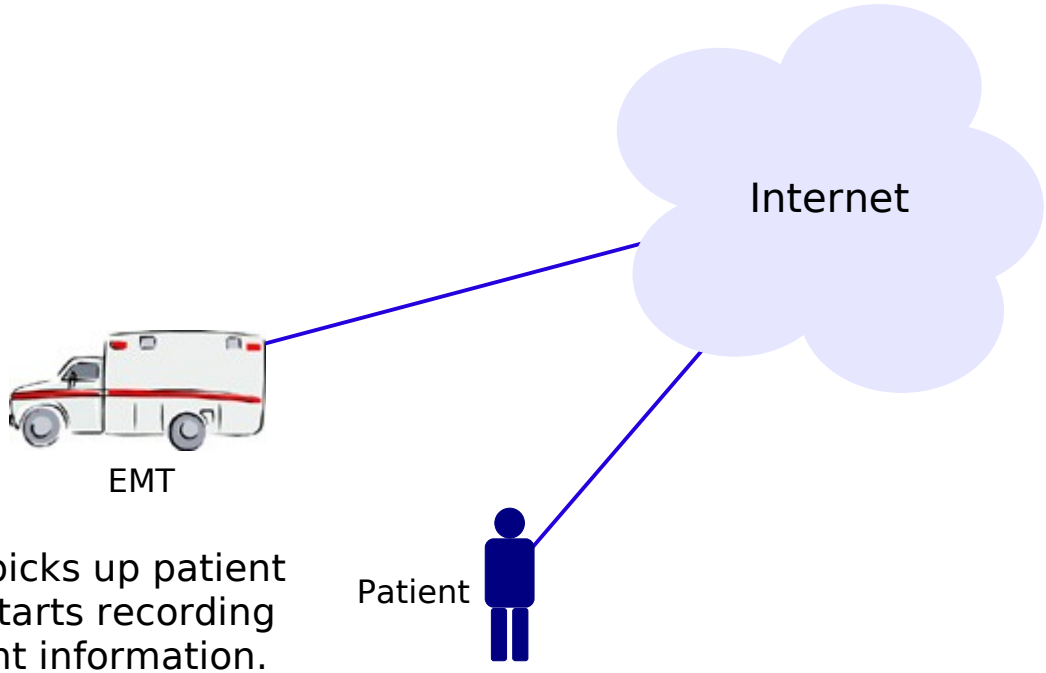
XML with XML Encryption

```
<?xml version="1.0" encoding="UTF-8"?>
<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
<ds:KeyInfo>
        <ds:KeyName>10514-1-1453</ds:KeyName>
        <ds:RetrievalMethod>http://localhost:8080/symkeyServlet/getsymkey</ds:RetrievalMethod>
        <ds:RetrievalMethod>http://skms.hospital.com/symkeyServlet/getsymkey</ds:RetrievalMethod>
</ds:KeyInfo>
<xenc:CipherData>
   <xenc:CipherValue>
        SID9GQ1rmuRBsIHcwK04TuGn4G8o2T99OaZtdT8BIH4rTT2YFT0a5D8FF9J0oFSJOXFLydpI8a4A
        DX7B/ZQCqa1VKhOnh0EfK0fjNfeuuw97yzTZyZ3y7uFQv1GJkqW7mBIzY9TKj4usTlOciEl1J5j1
        JwCTECcxDfb8/iKMW9GQXZzTOVjkWi+SSJSPeN1i0oZwY0o5zgVZESlV+71nDoVB2uM6p1BrM845
        jGqpuCr8gGaoD1GcF5sl2H9l4++JSmiZQZiapHvlEm3XbdsMRNsGYrVZhxbPWEvNiTuixBVJoXkx
        pY/z6pRrphzIwUCW88Ui5O7LhaBYbMepq1WJ0jyAEIaMc6LX8m8Hq+dneai2hBYSOqm0iSDInBeU
        VmkgwV7yzUBcxazr6Vdx3Z+xPI8TZtaSzffBldcGvaExQgdOhgzKNWyPUCt+NHRIBNj50XHiUcoR
        53NJd6u9YgjxL2pu48798OGmPzo7iTWd3Smj2nCoikJl2AL1xupl0hto8oBd42ltC27MDTdnSsp+
        SyeSLmnVoUwbo0DpGiwhl9pzU5IeDuKG7GYWIHG7zxJHvmiRzRmOjPZIFesXxIBT0UMdugew
   </xenc:CipherValue>
</xenc:CipherData>
<xenc:EncryptionProperties>
<xenc:EncryptionProperty name="InitializationVector">
        hAOPwhT0ocD4k7Jc
</xenc:EncryptionProperty>
</xenc:EncryptionProperties>
</xenc:EncryptedData>
```

Data & Key Classification

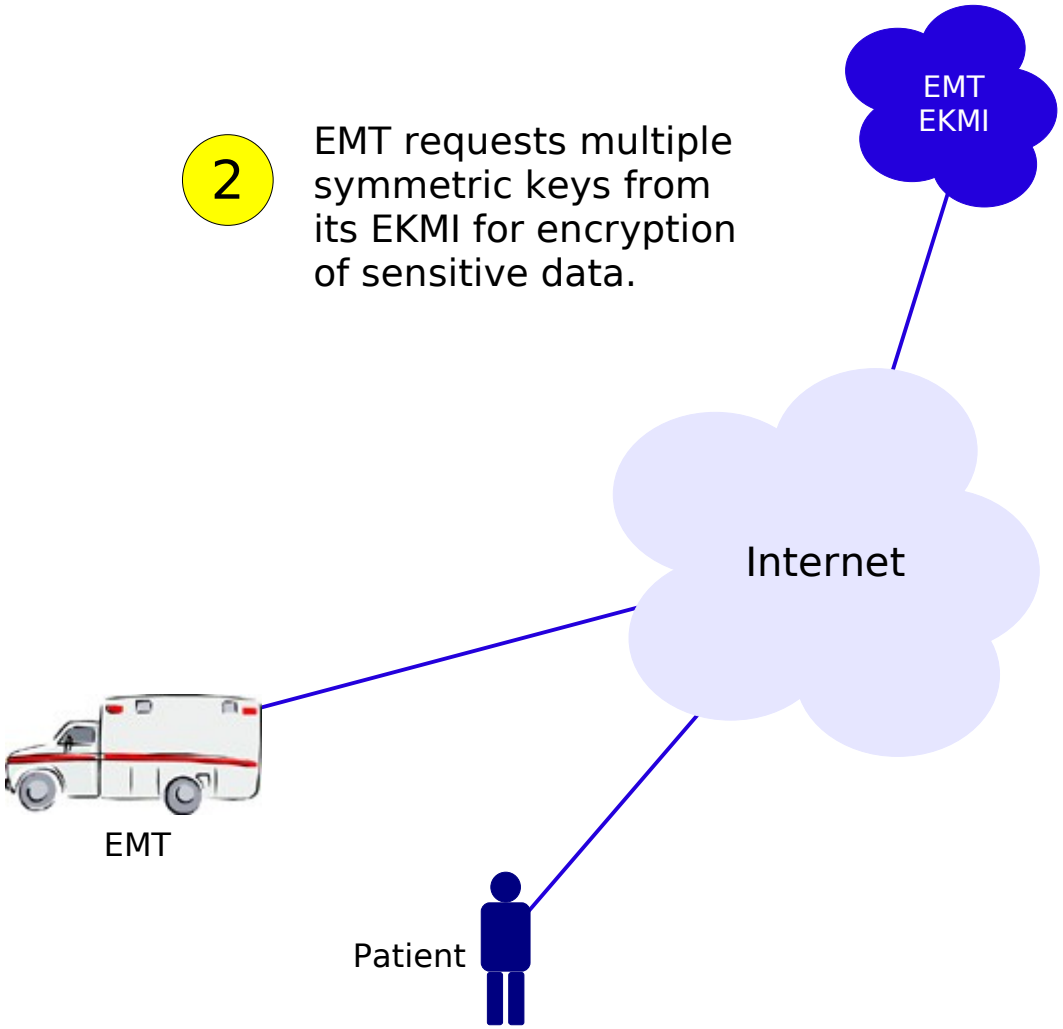
Data accessed by	Class
Center for Disease Control	EHR-CDC
Clinical Research Organization	EHR-CRO
Default access	EHR-DEF
Emergency Response Staff	EHR-EMT
Hospital Administration	EHR-HOS
Insurance Company	EHR-INS
Nursing Staff	EHR-NUR
Patient	EHR-PAT
Pharmacy	EHR-PHA
Physician	EHR-PHY

Event Flow - 1



1 EMT picks up patient and starts recording Patient information.

Event Flow - 2



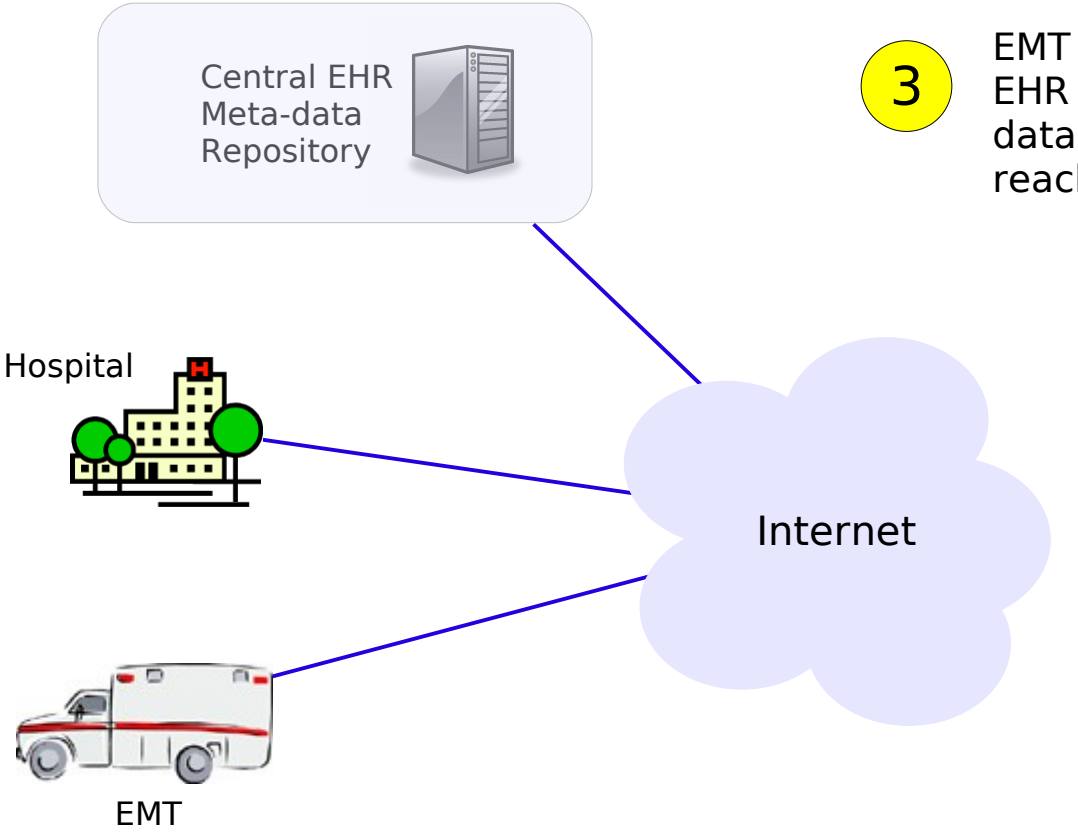
Symmetric Key Request

```
ekmi:SymkeyRequest xmlns:ekmi=”http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:GKID>10514-0-0</ekmi:GKID>
    <ekmi:KeyClasses>
        <ekmi:KeyClass>EHR-DEF</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-EMT</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-INS</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-PAT</ekmi:KeyClass>
    </ekmi:KeyClasses>
</ekmi:SymkeyRequest>
```

EKMI Response

```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:Symkey>
        <ekmi:GKID>10514-1-287</ekmi:GKID>
        .....
    </ekmi:Symkey>
    <ekmi:Symkey>
        <ekmi:GKID>10514-1-288</ekmi:GKID>
        .....
    </ekmi:Symkey>
    <ekmi:Symkey>
        <ekmi:GKID>10514-1-290</ekmi:GKID>
        .....
    </ekmi:Symkey>
    <ekmi:Symkey>
        <ekmi:GKID>10514-1-292</ekmi:GKID>
        .....
    </ekmi:Symkey>
</ekmi:SymkeyResponse>
```

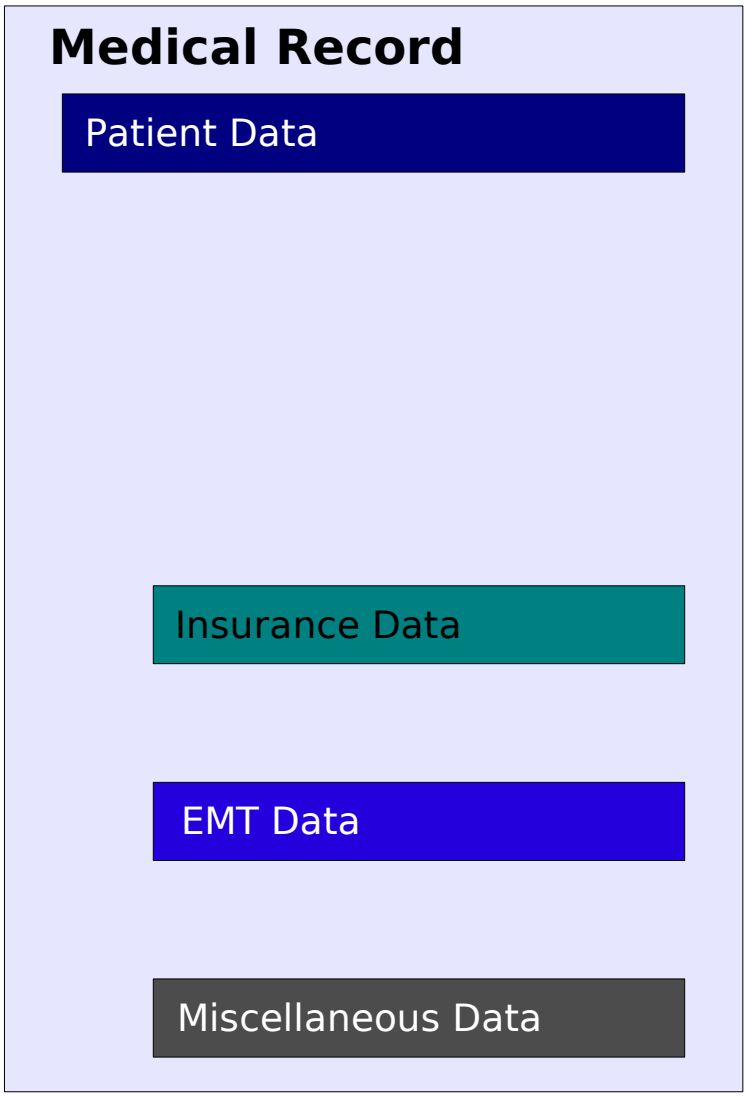
Event Flow - 3



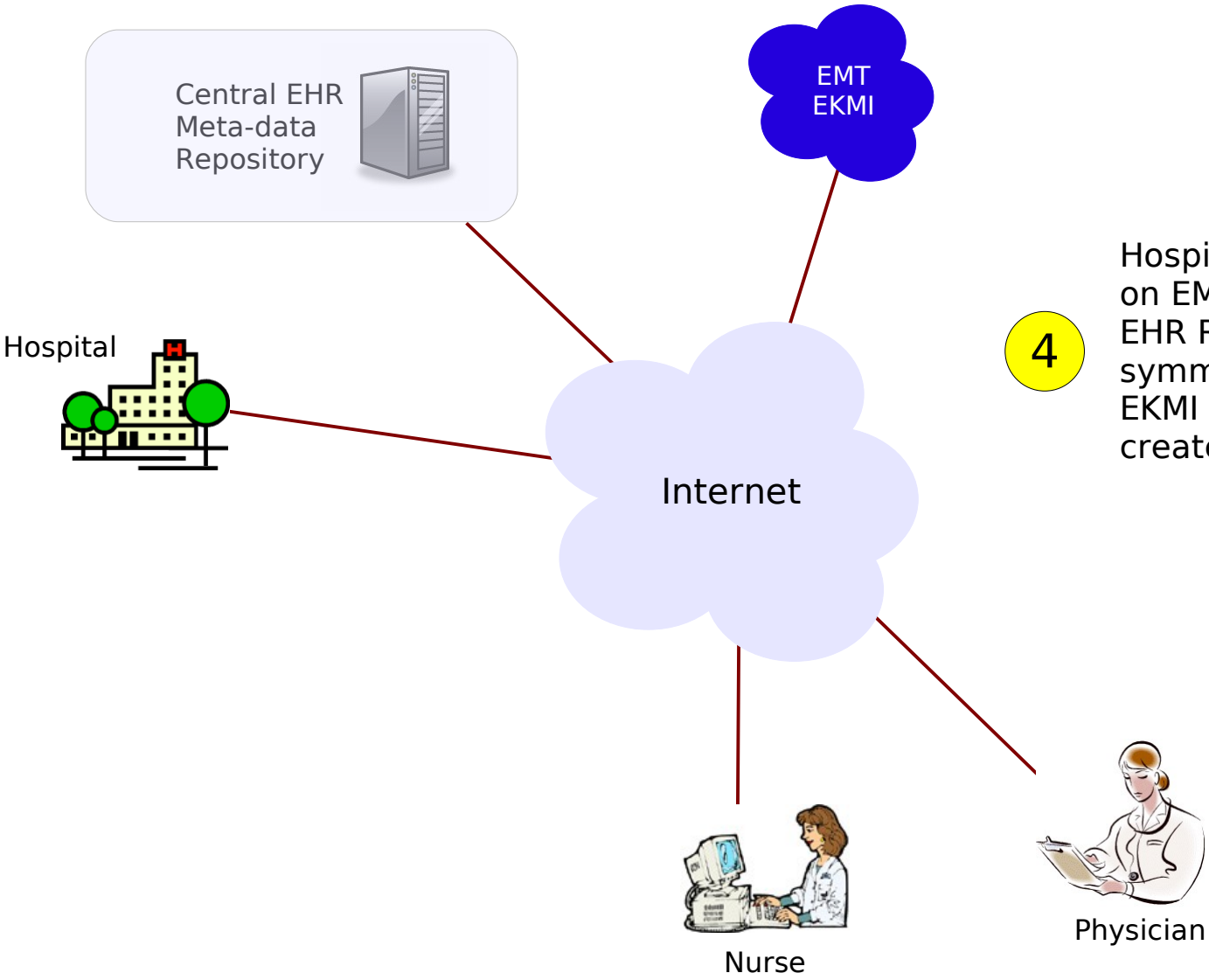
3

EMT updates Central EHR with new meta-data about event and reaches Hospital.

At this stage



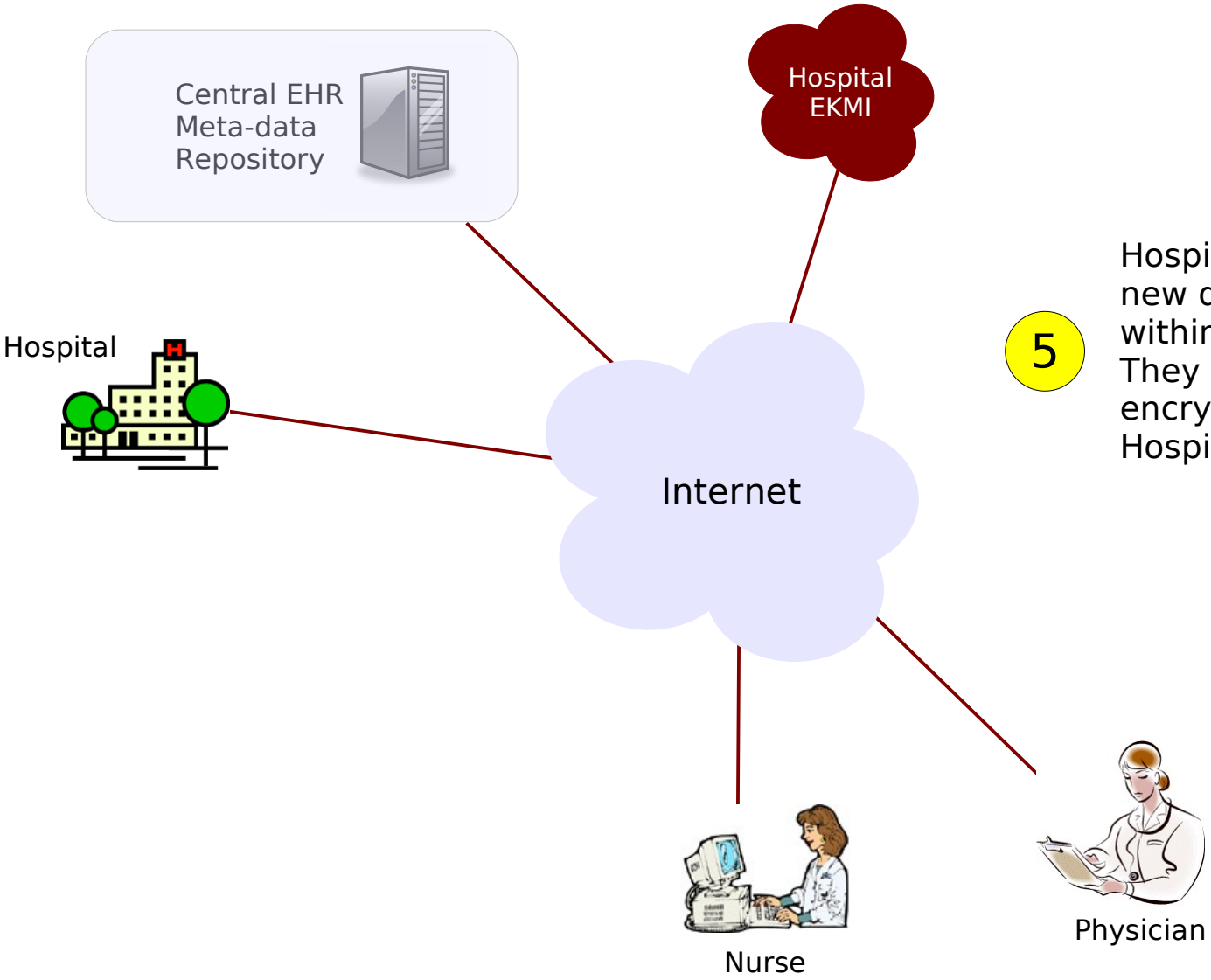
Event Flow - 4



Symmetric Key Request

```
ekmi:SymkeyRequest xmlns:ekmi=”http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:GKID>10514-1-287</ekmi:GKID>
    <ekmi:GKID>10514-1-288</ekmi:GKID>
    <ekmi:GKID>10514-1-290</ekmi:GKID>
    <ekmi:GKID>10514-1-292</ekmi:GKID>
</ekmi:SymkeyRequest>
```

Event Flow - 5



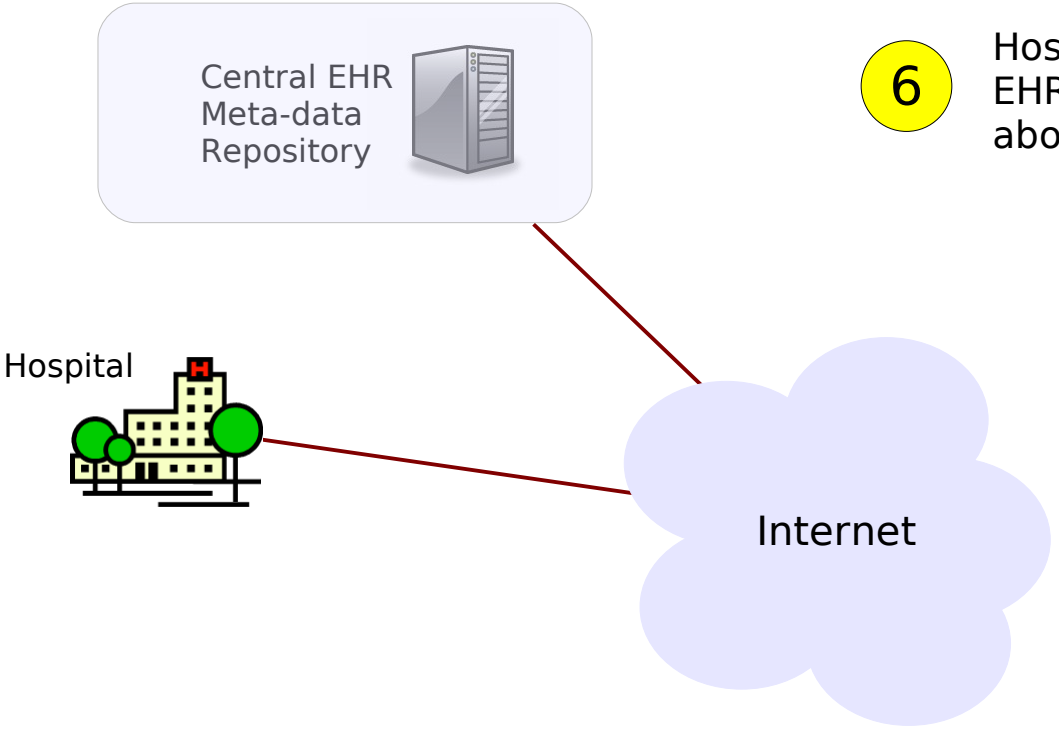
Symmetric Key Request

```
ekmi:SymkeyRequest xmlns:ekmi=”http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:GKID>5958-0-0</ekmi:GKID>
    <ekmi:KeyClasses>
        <ekmi:KeyClass>EHR-CDC</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-DEF</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-HOS</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-INS</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-NUR</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-PHA</ekmi:KeyClass>
        <ekmi:KeyClass>EHR-PHY</ekmi:KeyClass>
    </ekmi:KeyClasses>
</ekmi:SymkeyRequest>
```

EKMI Response

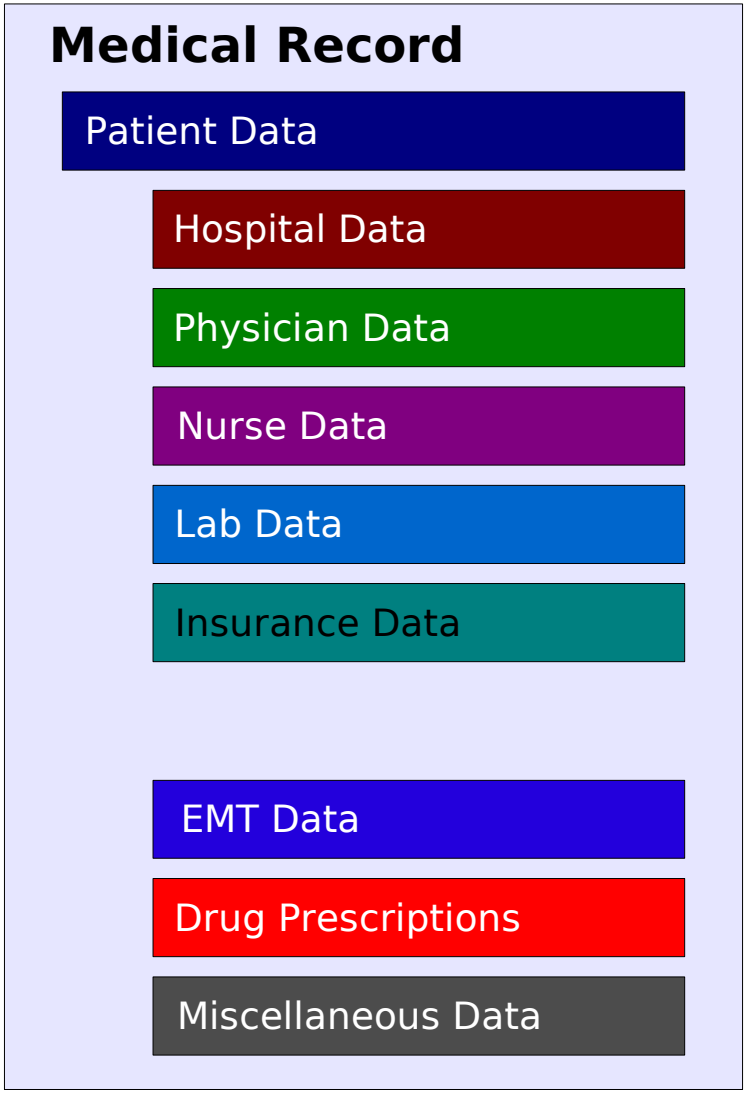
```
<ekmi:SymkeyResponse
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:ekmi="http://docs.oasis-open.org/ekmi/2008/01">
    <ekmi:Symkey>
        <ekmi:GKID>5958-4-87234</ekmi:GKID>
        .....
    </ekmi:Symkey>
    <ekmi:Symkey>        .....        </ekmi:Symkey>
    <ekmi:Symkey>        .....        </ekmi:Symkey>
    <ekmi:Symkey>        .....        </ekmi:Symkey>
    <ekmi:Symkey>        .....        </ekmi:Symkey>
    <ekmi:Symkey>        .....        </ekmi:Symkey>
    <ekmi:Symkey>        .....        </ekmi:Symkey>
</ekmi:SymkeyResponse>
```

Event Flow - 6

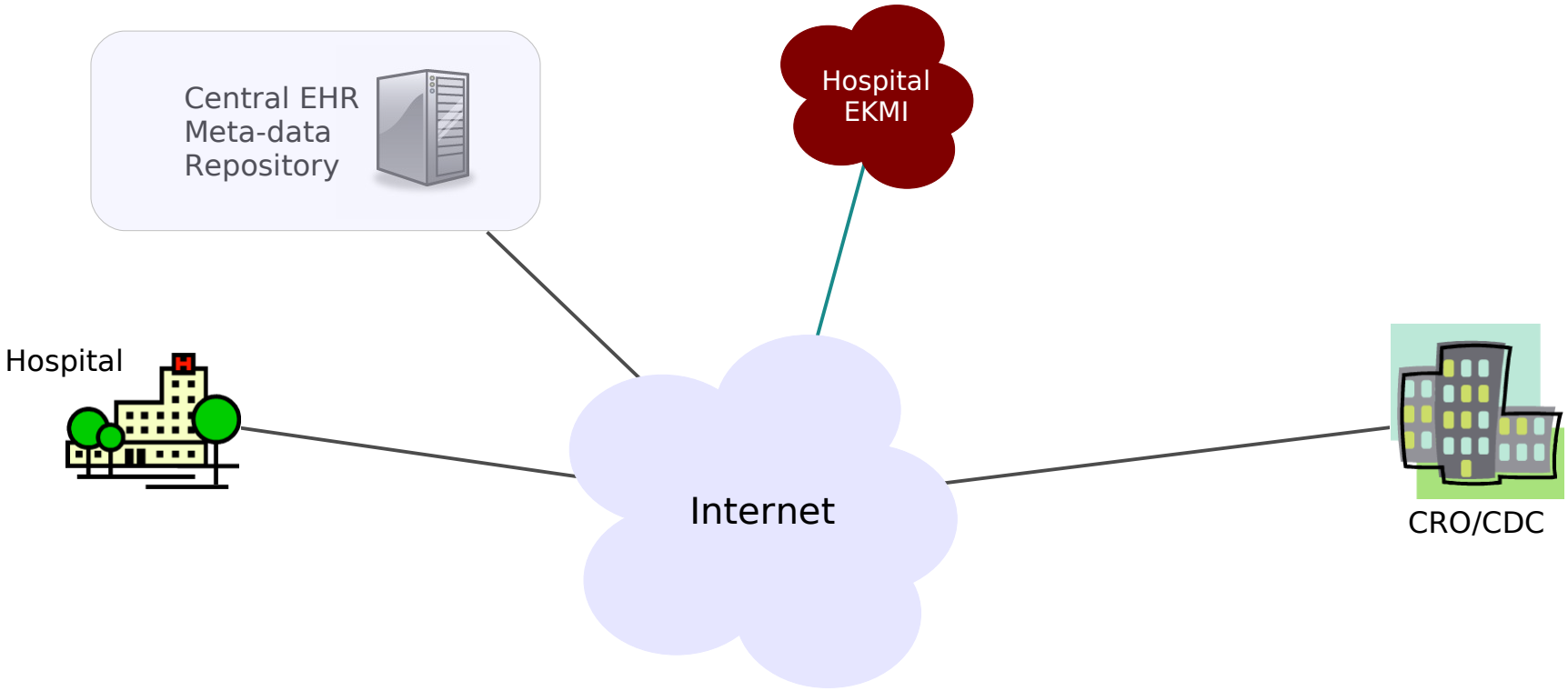


6 Hospital updates Central EHR with new meta-data about event.

At this stage

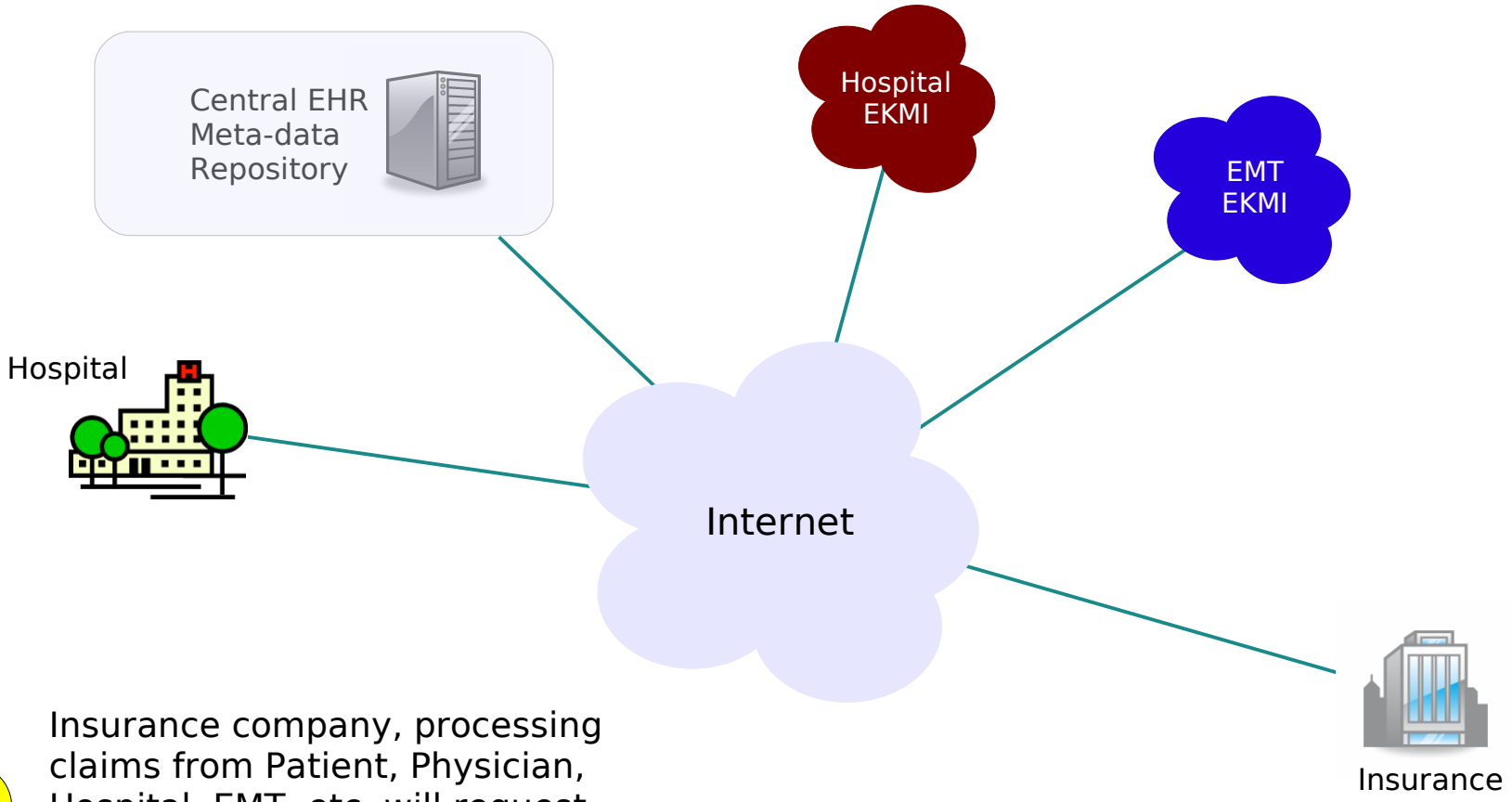


Event Flow - 7



7 Depending on Patient's illness, CDC may receive notification and based on Central EHR data request symmetric keys from Hospital EKMI to decrypt data.

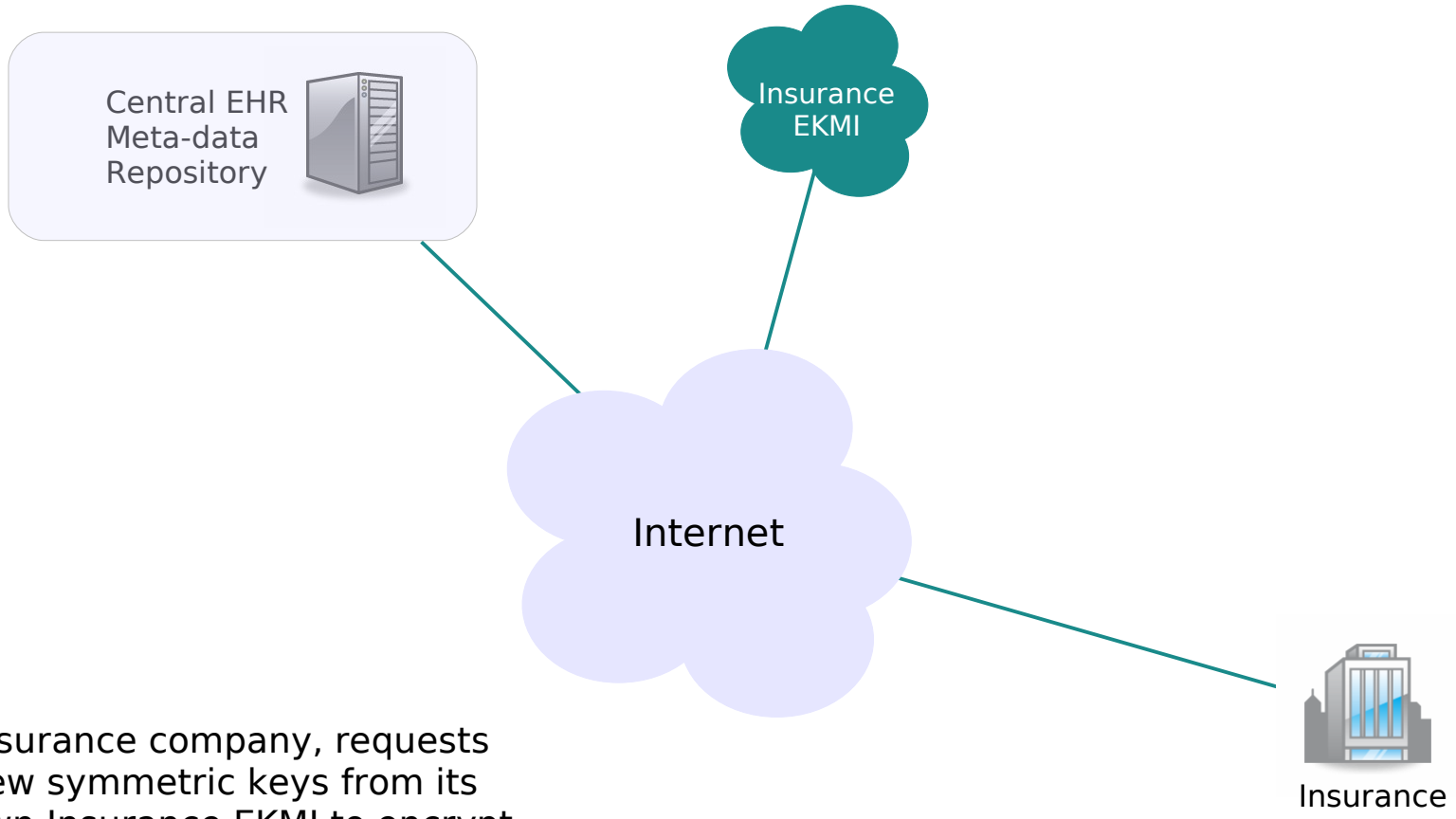
Event Flow - 8



8

Insurance company, processing claims from Patient, Physician, Hospital, EMT, etc. will request symmetric keys from Hospital's and EMT's EKMI to decrypt data it needs for claims-processing.

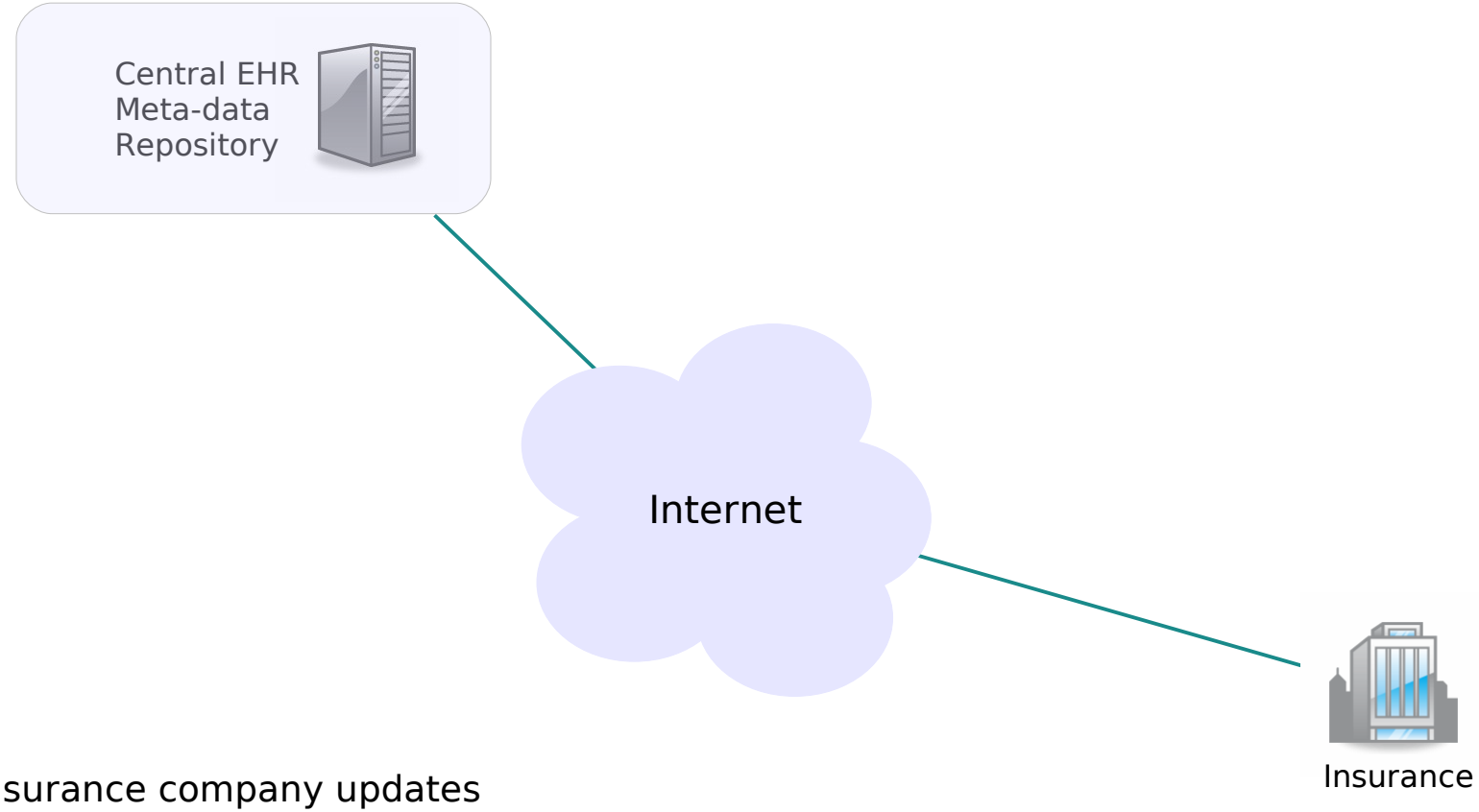
Event Flow - 9



9

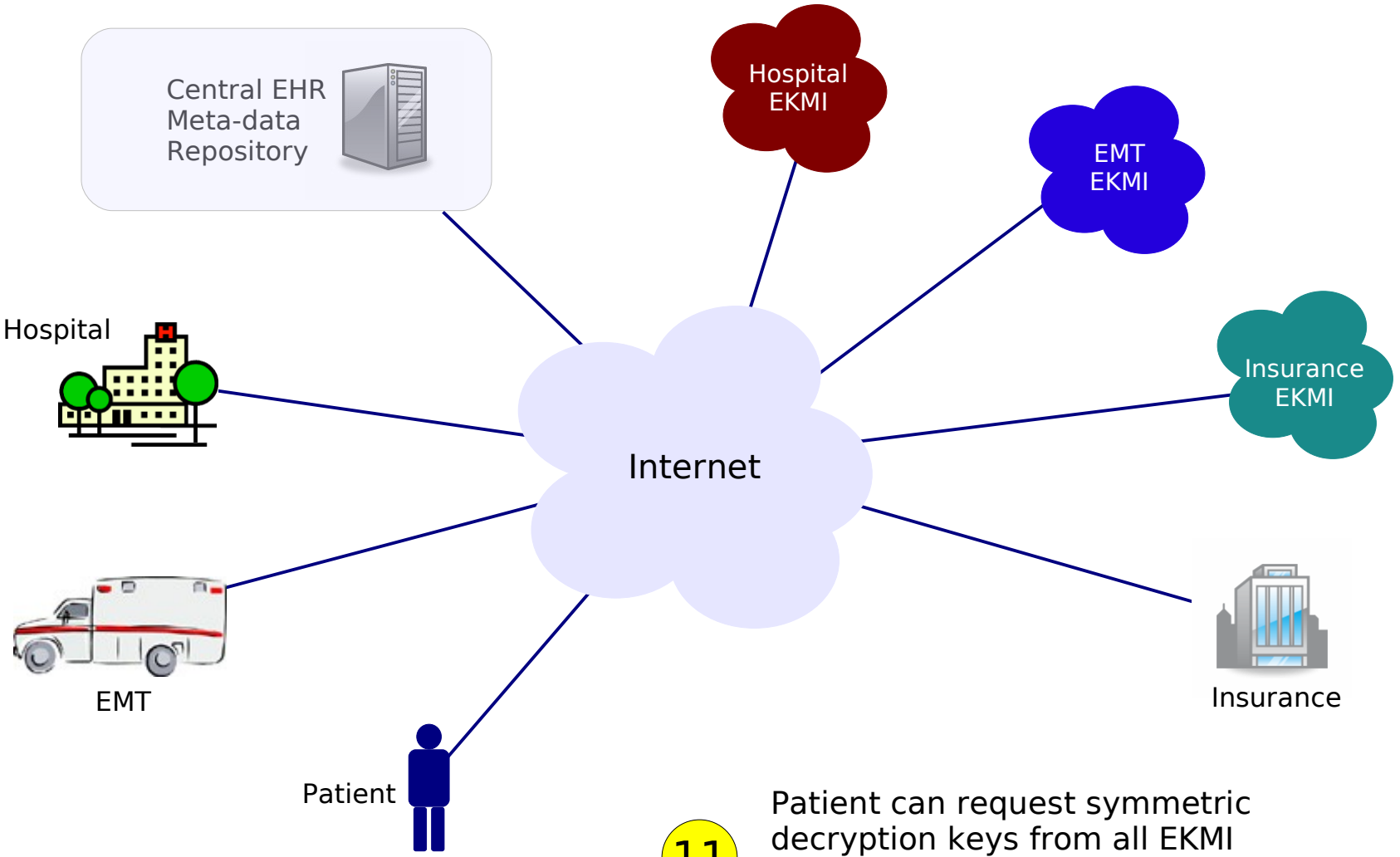
Insurance company, requests new symmetric keys from its own Insurance EKMI to encrypt sensitive data about the event and its processing.

Event Flow - 10



10 Insurance company updates Central EHR Meta-Repository with claims data.

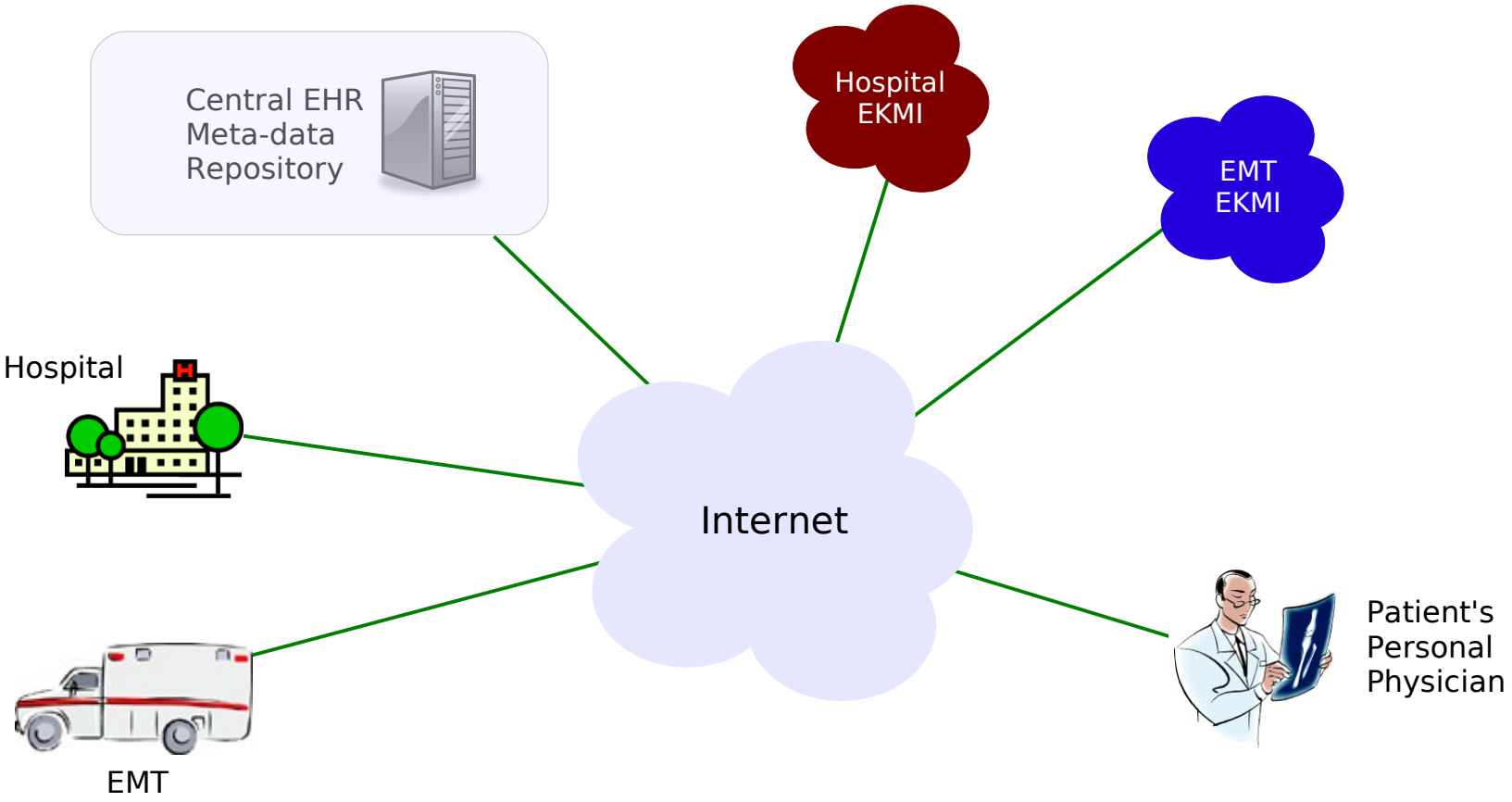
Event Flow - 11



11

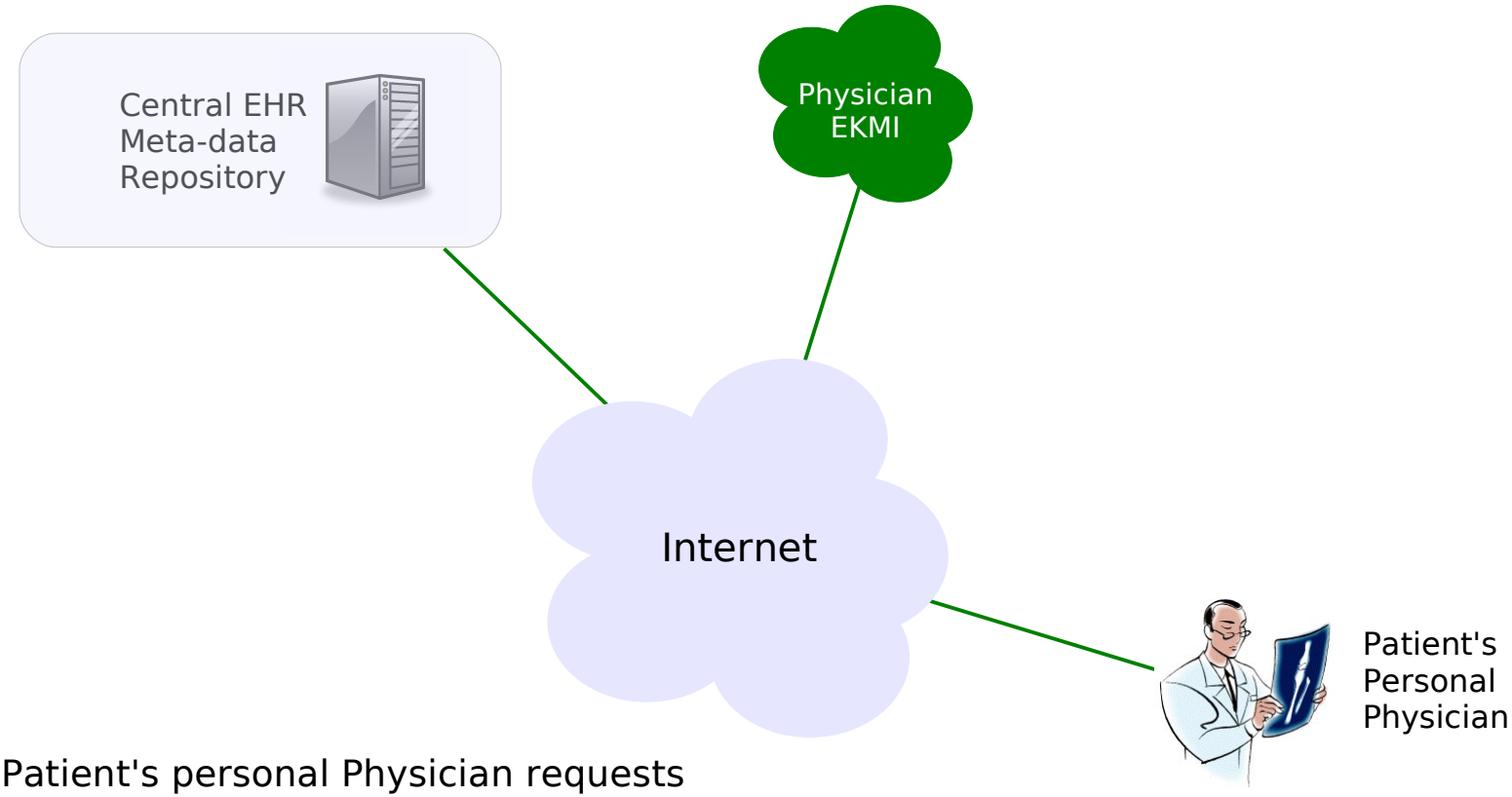
Patient can request symmetric decryption keys from all EKMI and view their medical history as desired.

Event Flow - 12



12 Patient's personal Physician can request symmetric keys from Hospital and EMT EKMI to review medical data.

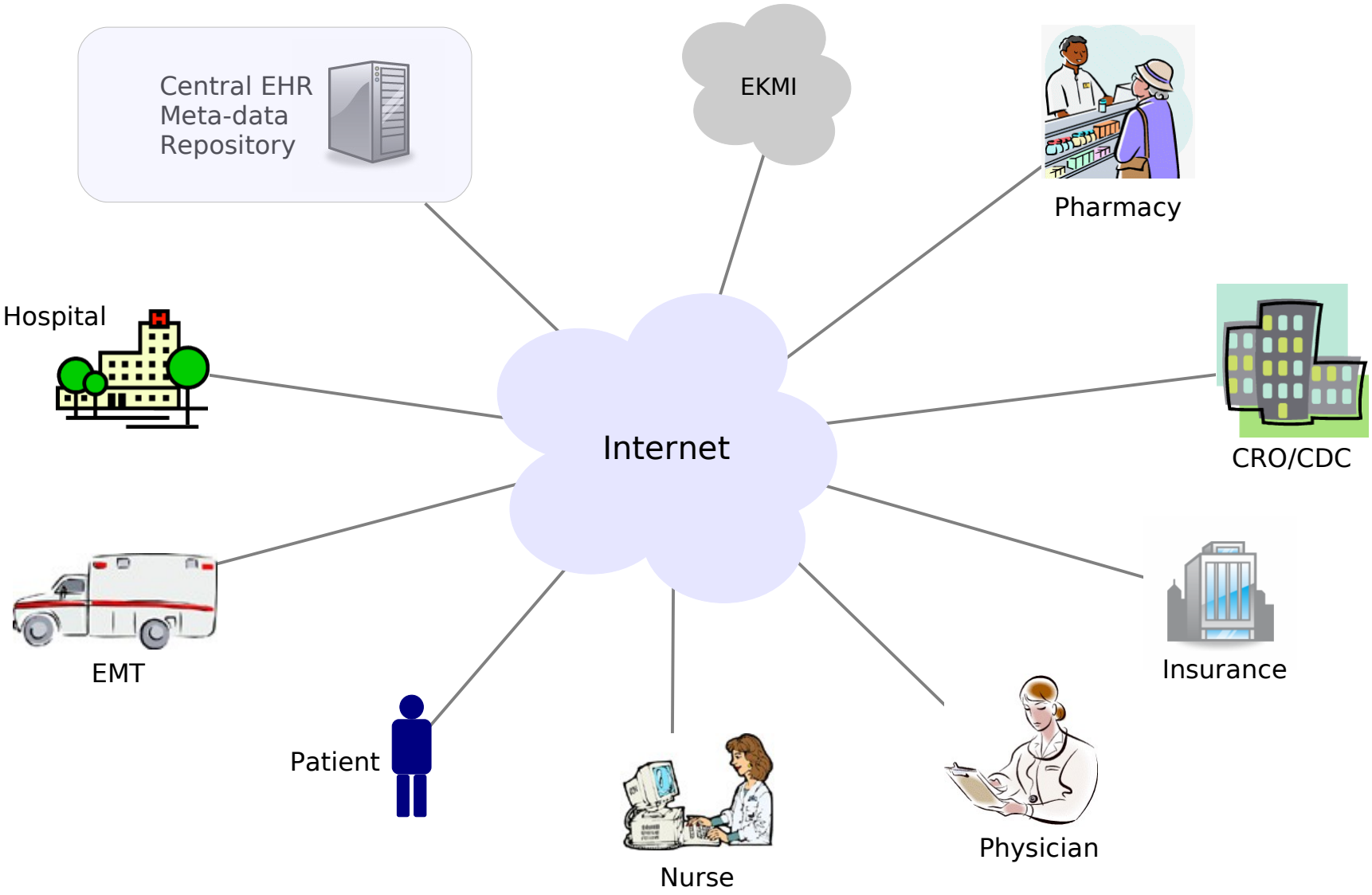
Event Flow - 13



13

Patient's personal Physician requests new symmetric encryption keys from Physician's EKMI (perhaps provided by a service-provider) to encrypt new medical information. Central EHR repository is updated subsequently.

Is this feasible?



YES – with an EKMI

- All medical data can be encrypted
- All data can be accessible over the internet
- Symmetric keys are accessible only with strong authentication and is role-based
- All authorized entities can retrieve the keys they need to perform their function
- Authorized entities can retrieve only the keys they need based on preassigned key-classes
- All keys are protected by hardware cryptographic tokens such as HSM, smartcards, TPMs, etc.
- Network and Host security is redundant

Conclusion

- Questions?
- Contact Information
  - www.strongauth.com
  - www.strongkey.org
  - info@strongauth.com
  - (408) 331-2000