HIMSS14
Annual Conference & Exhibition

FEBRUARY 23–27, 2014
ORLANDO, FLORIDA

INNOVATION. IMPACT. OUTCOMES.
ONWARD

A Lightweight, Decentralized Trust Framework for DIRECT Messaging

February 24, 2014

Walter Sujansky, MD PhD

President, Sujansky & Associates LLC

Conflict of Interest Disclosure

Dr. Sujansky's firm, Sujansky & Associates, earns fees for its planning, implementation, and operation of DIRECT messaging infrastructures in medical communities

HIMSS14
ANNUAL CONFERENCE & EXHIBITION

Learning Objectives

- Understand **the practical challenges of establishing trust** among healthcare organizations that wish to exchange protected health information (PHI) through **DIRECT messaging**
- **Review a number of approaches** that have been attempted in the past to close the “trust gap” for health information exchange **and why no approach has yet succeeded** on a large scale
- **Consider a novel trust framework for DIRECT messaging** that combines elements of current approaches with **new technical, operational, and legal constructs** that provide greater decentralization and scalability

.

The Healthcare Benefits of a Decentralized and Scalable Trust Framework for DIRECT Messaging

- Secure exchange of patient health information as ubiquitously and conveniently as conventional email messaging
- Low-cost, low-overhead communication channel for many of the Stage-2 M.U. measures that require interoperability, including:
  - Transitions of care and referrals
  - Delivery of structured lab results
  - Submission of data to immunization registries
- Improved care coordination among all clinical settings, regardless of type, size, or business affiliation

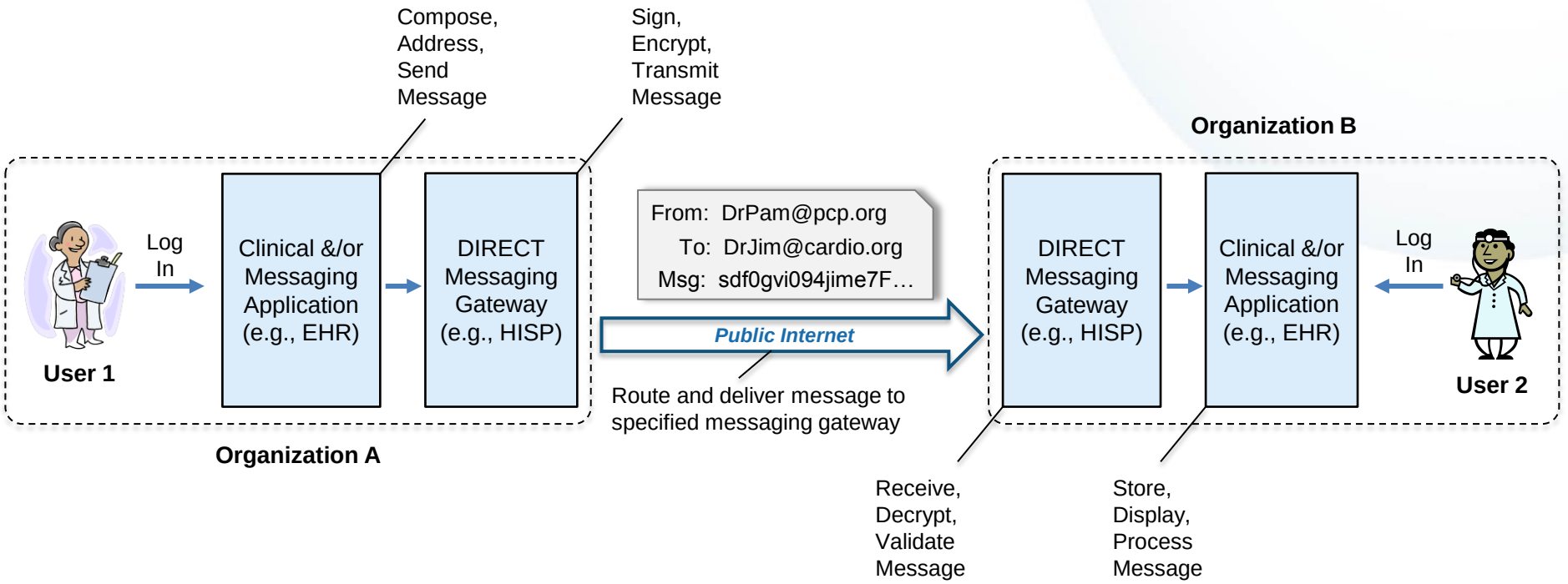
DIRECT Messaging for Health Information Exchange

DIRECT Messaging is…

- A secure messaging protocol based on mature industry standards
  - SMTP (transport), MIME (payload), PKI (encryption/signature)
- Similar to email
  - Senders and recipients are defined and located by email addresses, such as JamesMorrisMD@direct.cardioassociates.org
  - Messages can contain text or html contents, as well as arbitrary (MIME) attachments, such as XML, HL7, PDF, images
- Applicable beyond "human-to-human" messaging
  - Machine-to-human (PDF discharge summary)
  - Machine-to-machine (HL7 lab result)
- Non-proprietary => May be and has been implemented by many vendors
- Readily interoperable => mature standards, open-source implementation

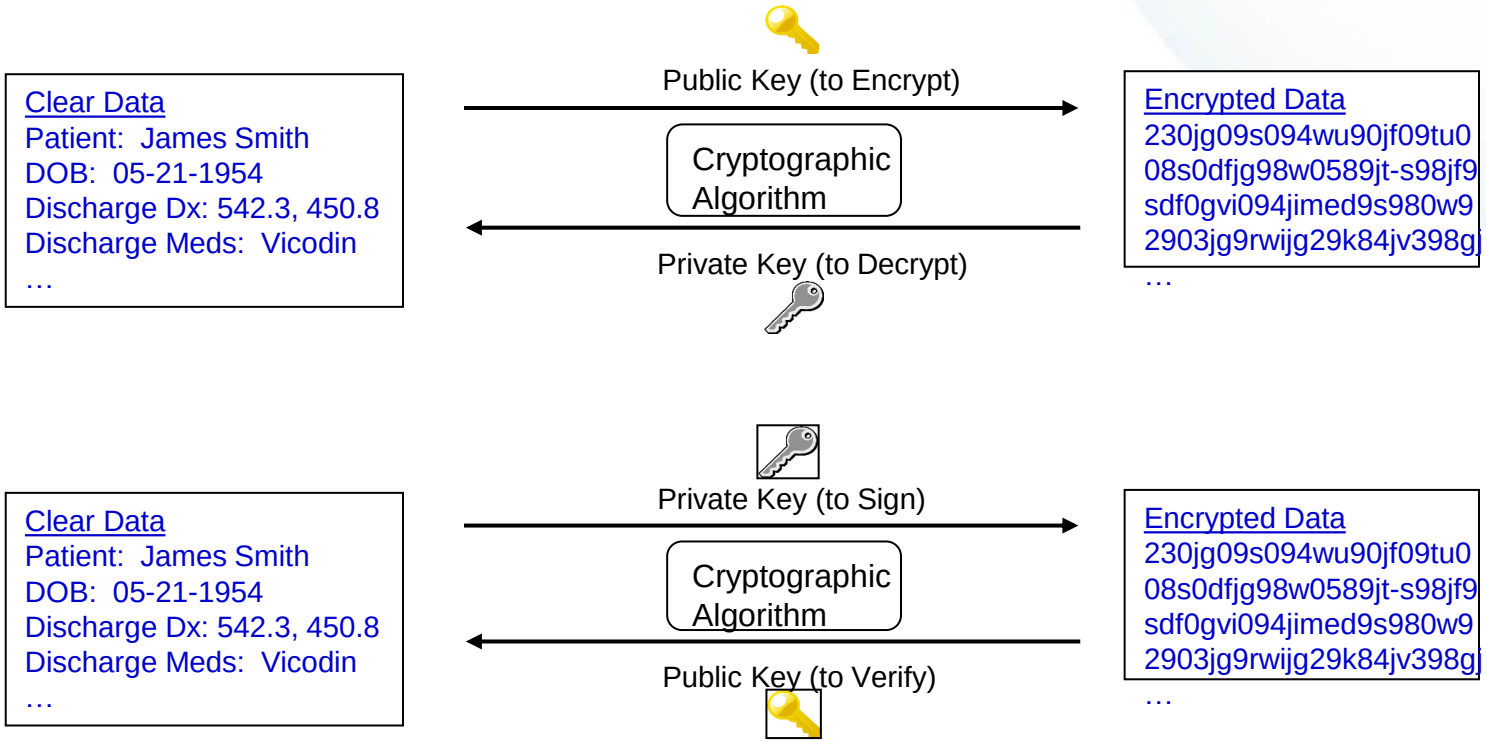
DIRECT Messaging for Health Information Exchange

DIRECT Messaging is…



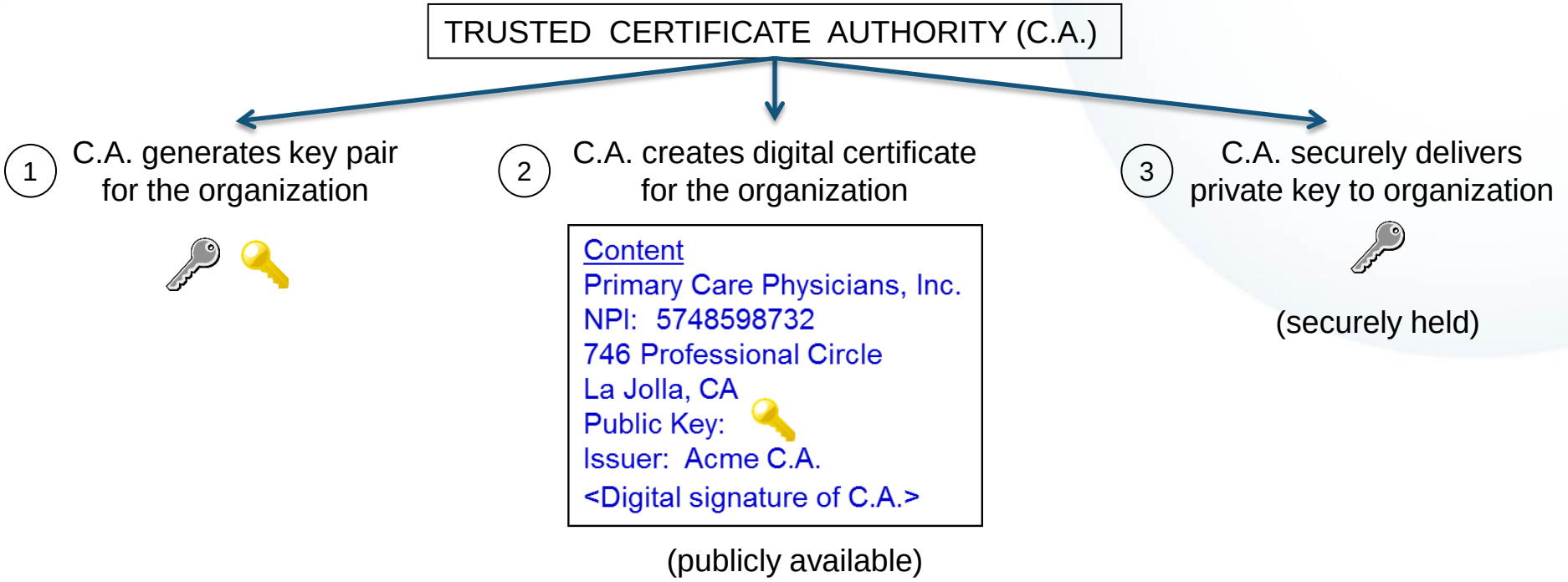
Public Key Infrastructure (PKI)

- Data encryption based on two complementary cryptographic keys:
  - Private Key – Held by assigned party only
  - Public Key – Available to everyone else



Public Key Infrastructure (PKI)

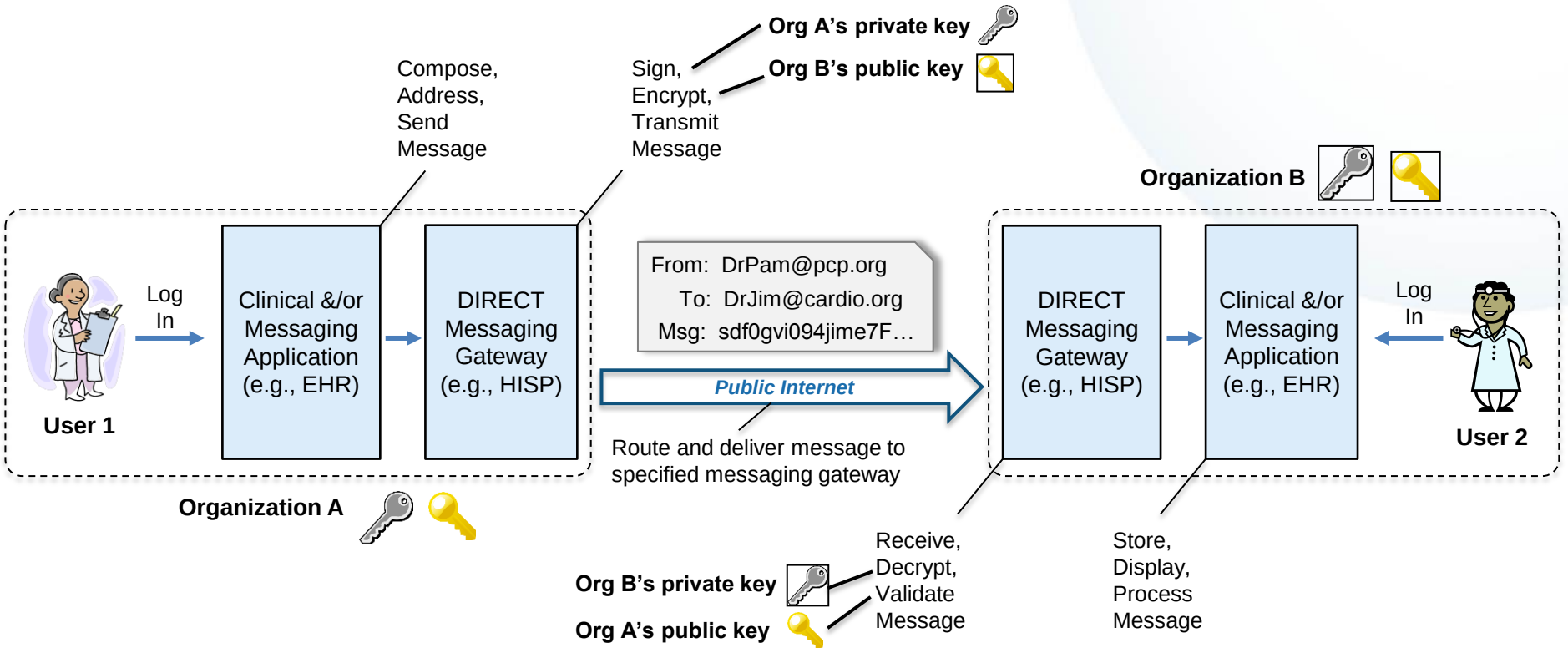
- Digital Certificates



- Meaning: The Certificate Authority has validated that the organization:
  - Legitimately exists and has the attributes listed
  - Was provided the private key that corresponds to the listed public key

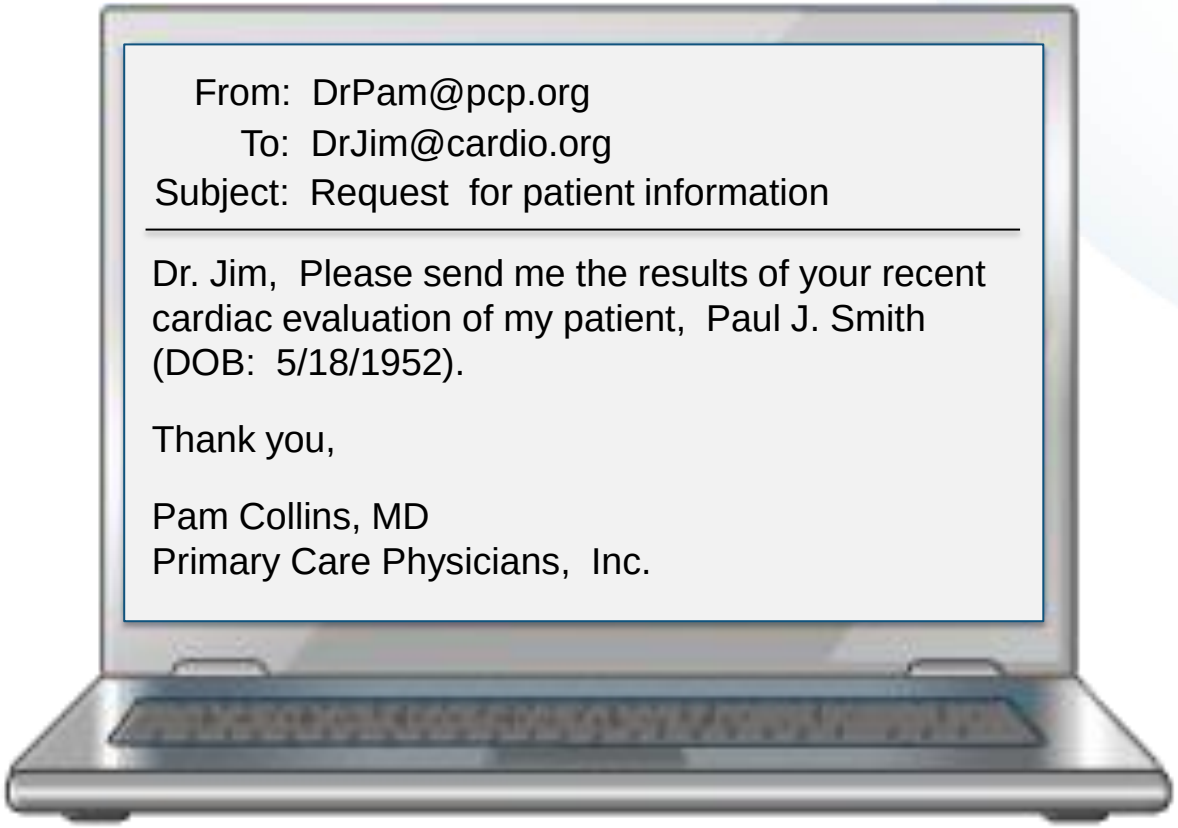
Public Key Infrastructure (PKI)

- Encryption and Signing of DIRECT messages



Challenges to Establishing Trust in DIRECT Messaging

Imagine you receive the following DIRECT message:



Do you respond?

Challenges to Establishing Trust in DIRECT Messaging

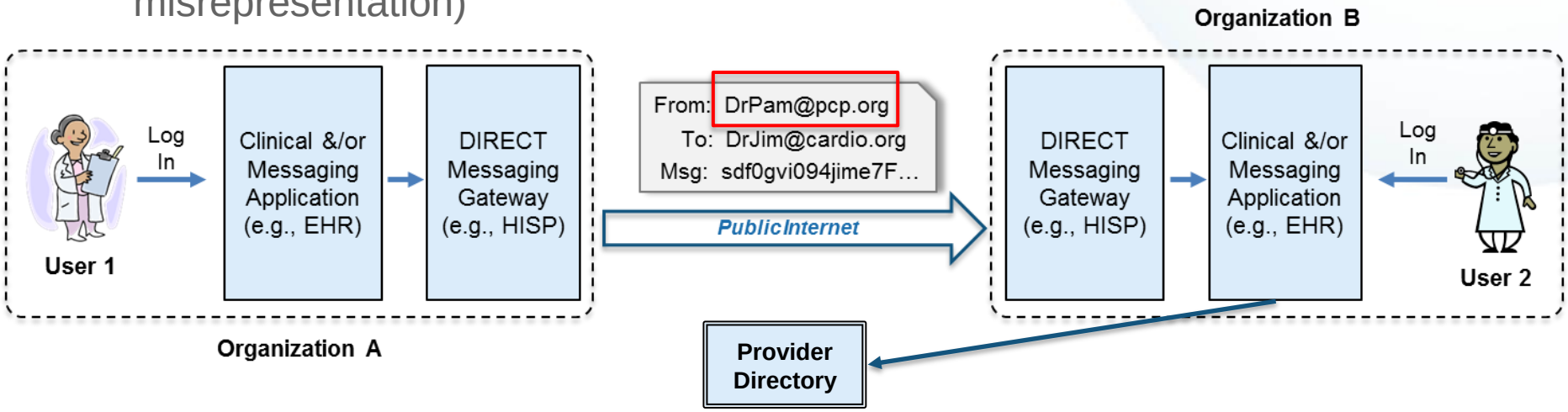
What is the opposite of Trust?

Risk

Challenges to Establishing Trust in DIRECT Messaging

1. Address Risk

- The DIRECT email address to which PHI will be sent is not the correct address of the intended or represented recipient (due to error or malicious misrepresentation)

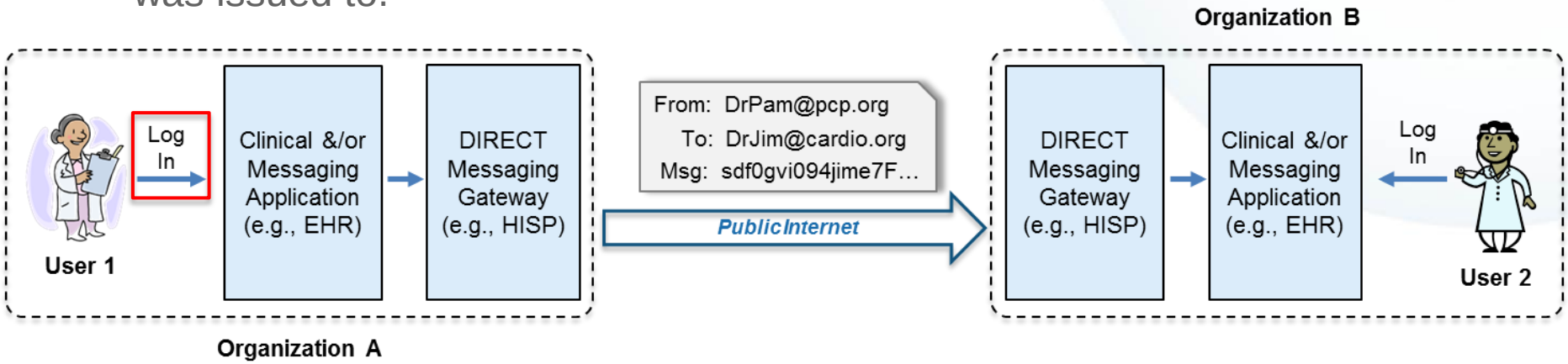


- Solution(s)
  - Trusted digital certificates for organizations
  - Trusted provider directory(ies) for individuals

Challenges to Establishing Trust in DIRECT Messaging

2. Authentication Risk

- A DIRECT email account is accessed by someone other than the person it was issued to.



- Solution(s)
  - Reliable authentication mechanisms, including complex passwords, password expiration policies, and/or two-factor authentication
  - Secure delivery of authentication credentials to users

Challenges to Establishing Trust in DIRECT Messaging

3. Identity Risk

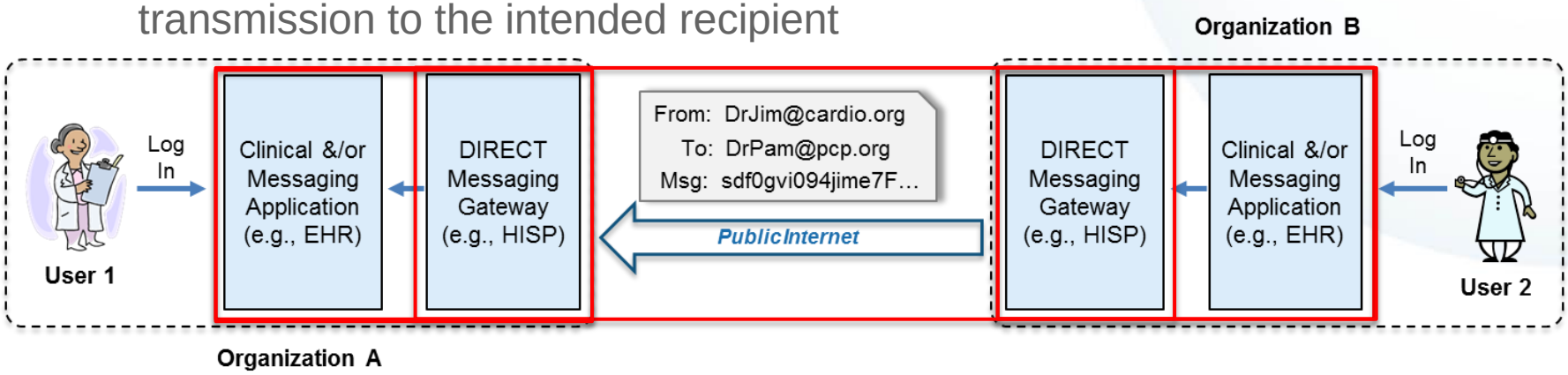
- The DIRECT email address and account for a specific provider were issued to a different person who successfully claimed to be the provider and was issued an account in her name.

- Solution(s)
  - Robust identity proofing at the time that accounts are created for providers

Challenges to Establishing Trust in DIRECT Messaging

4. Disclosure Risk

- PHI within a message is disclosed to an unauthorized party during transmission to the intended recipient

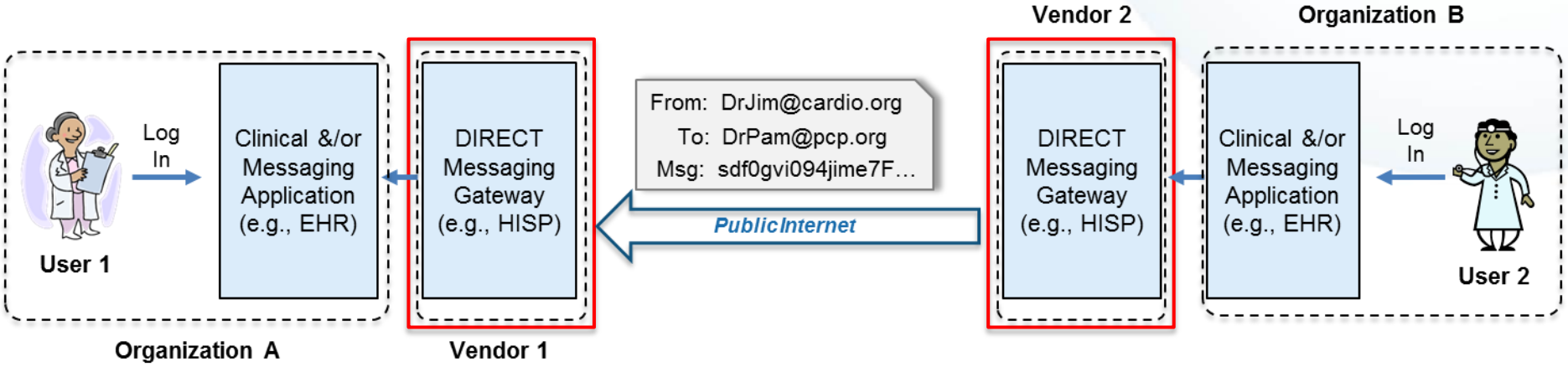


- Solution(s)
  - Reliable encryption of message contents over public internet
  - Reliable safeguarding of private decryption keys by intended recipient
  - Appropriate technical safeguards for DIRECT message gateways and clinical / messaging applications to prevent intrusion

Challenges to Establishing Trust in DIRECT Messaging

5. Agency Risk

- A third party that handles the encryption, decryption, and/or storage of DIRECT messages on behalf of a healthcare organization does not have sufficiently secure technology and processes

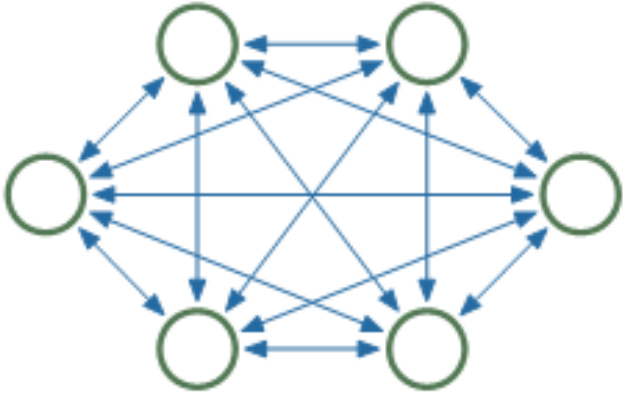


- Solution(s)
  - Binding contractual agreements with third parties (e.g., BAAs)
  - Formal accreditation of third parties by trusted entities

Approaches to Establishing Trust

1. Pairwise Contracts between Provider Organizations

- Negotiation of mutually agreeable policies and practices for assigning addresses, authenticating users, securing information systems, using transmitted PHI, and remediating adverse events



Approaches to Establishing Trust

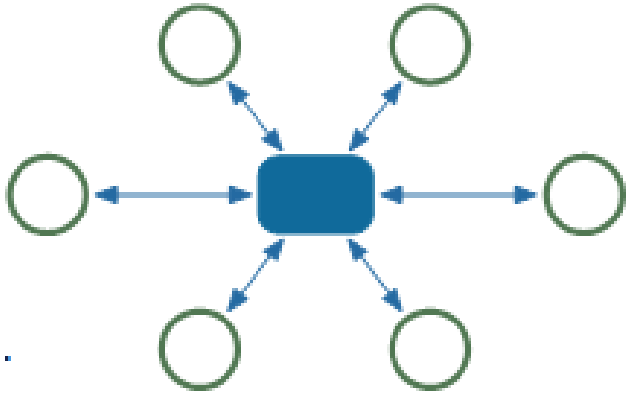
1. Pairwise Contracts between Provider Organizations

- Negotiation of mutually agreeable policies and practices for assigning addresses, authenticating users, securing information systems, using any transmitted PHI, and remediating adverse events
- Pros
  - Terms customized to the requirements/constraints of each party
  - All parties feel comfortable and protected
- Cons
  - Each organization must negotiate and execute such an agreement separately with every other organization => ~ N-Squared agreements
  - Terms of each agreement will vary
  - Very costly and time consuming process, which may be feasible for only the largest and most motivated trading partners => closed system

Approaches to Establishing Trust

2. A Mutual Contract for All Provider Organizations

- Each organization executes the same contract with a third party, binding them all to a common set of policies and practices for assigning addresses, authenticating users, securing information systems, using transmitted PHI, and remediating adverse events



Approaches to Establishing Trust

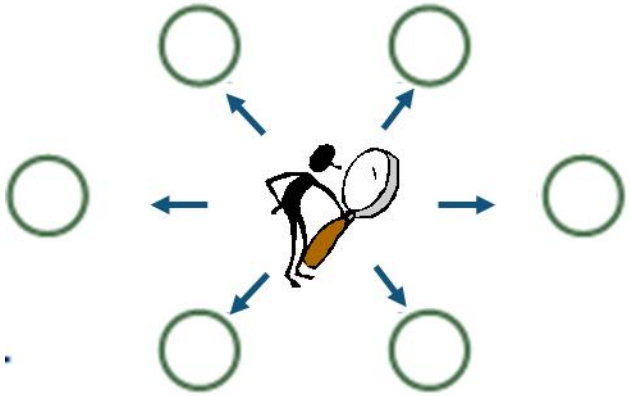
2. A Mutual Contract for All Provider Organizations

- Each organization executes the same contract with a third party, binding them all to a common set of policies and practices for assigning addresses, authenticating users, securing information systems, using transmitted PHI, and remediating adverse events
- Pros
  - Only one agreement needs to be created/negotiated, saving cost and time
- Cons
  - Who is the third party for DIRECT messaging?
  - It may be difficult/impossible to craft a single binding agreement that is acceptable to all provider organizations in a community
  - Any exceptions/variances will require organizations to review/understand all other organizations' contracts

Approaches to Establishing Trust

3. Best Practices and Third-party Accreditation

- Instead of relying on binding contracts, participating organizations base their trust on the formal accreditation of other organizations with respect to an externally defined set of best practices for assigning addresses, authenticating users, securing information systems, etc.



Approaches to Establishing Trust

3. Best Practices and Third-party Accreditation

- Instead of relying on binding contracts, participating organizations base their trust on the formal accreditation of other organizations with respect to an externally defined set of best practices for assigning addresses, authenticating users, securing information systems, etc.
- Pros
  - No contract negotiations required for pairwise or mutual contracts
  - Some validation of adherence to best practices
  - Provider organizations can outsource to accredited vendors
- Cons
  - Liability in the case of adverse events is uncertain => Provider organization? Vendor? Accrediting body?
  - Defined best practices may be unnecessarily detailed/prescriptive

Approaches to Establishing Trust: DirectTrust.org

- DT.org has defined a set of best practices with respect to:
  - Registration Authorities (RAs)
    - Identity proofing of organizations and individuals participating in DIRECT
  - Certificate Authorities (CAs):
    - Secure generation of digital certificates and distribution of private keys
    - Revocation of digital certificates when necessary
  - Health Information Service Providers (HISPs):
    - Encryption/validation of DIRECT messages when they are sent and received
    - Secure management of private keys for encryption/signing
- DT.org oversees accreditation program for RAs, CAs, and HISPs
- DT.org manages “Trust Bundle” containing certificates of all accredited HISPs
  - May be used by HISPs to constrain DIRECT messaging only to other accredited HISPs

DirectTrust.org

- DirectTrust.org is an excellent general approach to underpinning trust in DIRECT messaging
  - Defines clear and robust best practices based on industry standards
  - Helps to educate vendors and provider organizations through its accreditation process
  - Effectively supports a model of DIRECT messaging that is HISP-centric and assumes individual provider certificates

Approaches to Establishing Trust: DirectTrust.org

- The DirectTrust.org accreditation model alone may not result in the scalable and ubiquitous trust framework that is envisioned
  - Perhaps not sufficient
    - Lack of a clear and accepted legal foundation for transmission of PHI based solely on DirectTrust.org accreditation
    - Incomplete assurance of security for sender and recipient addresses, identity, and authentication when *organization*, rather than individual, certificates are used by DIRECT gateways (and this will likely be the norm)
  - Perhaps not wholly necessary
    - Covered entities and their contracted agents (BAs) are already subject to the provisions of the HIPAA Privacy and Security Rules (which require secure handling of PHI when “received or transmitted”)
    - Requirement for accreditation with respect to the highly detailed and prescriptive best practices defined by DirectTrust.org may impede adoption of DIRECT messaging among all organizations

Approaches to Establishing Trust: A Supplemental Model

- Legal Foundation: HIPAA Security and Privacy Rules
  - Already familiar to provider organizations and their attorneys
  - Place ultimate responsibility for and control of the secure transmission/receipt of PHI on covered entities
    - CEs subsequently pass this responsibility (via BAAs) on to any agents who transmit/receive PHI on their behalf (such as HISPs)
- Technical Mechanisms:
  - Digital certificates and private keys issued to covered entities
  - Digital "security assertions" signed by covered entities, which attest to:
    - The identity of any senders of DIRECT messages originating from the covered entity ("Authentication Assertions")
    - The validity of any DIRECT addresses published by the covered entity ("Address Assertions")

Approaches to Establishing Trust: A Supplemental Model

Security Assertion Markup Language (SAML)

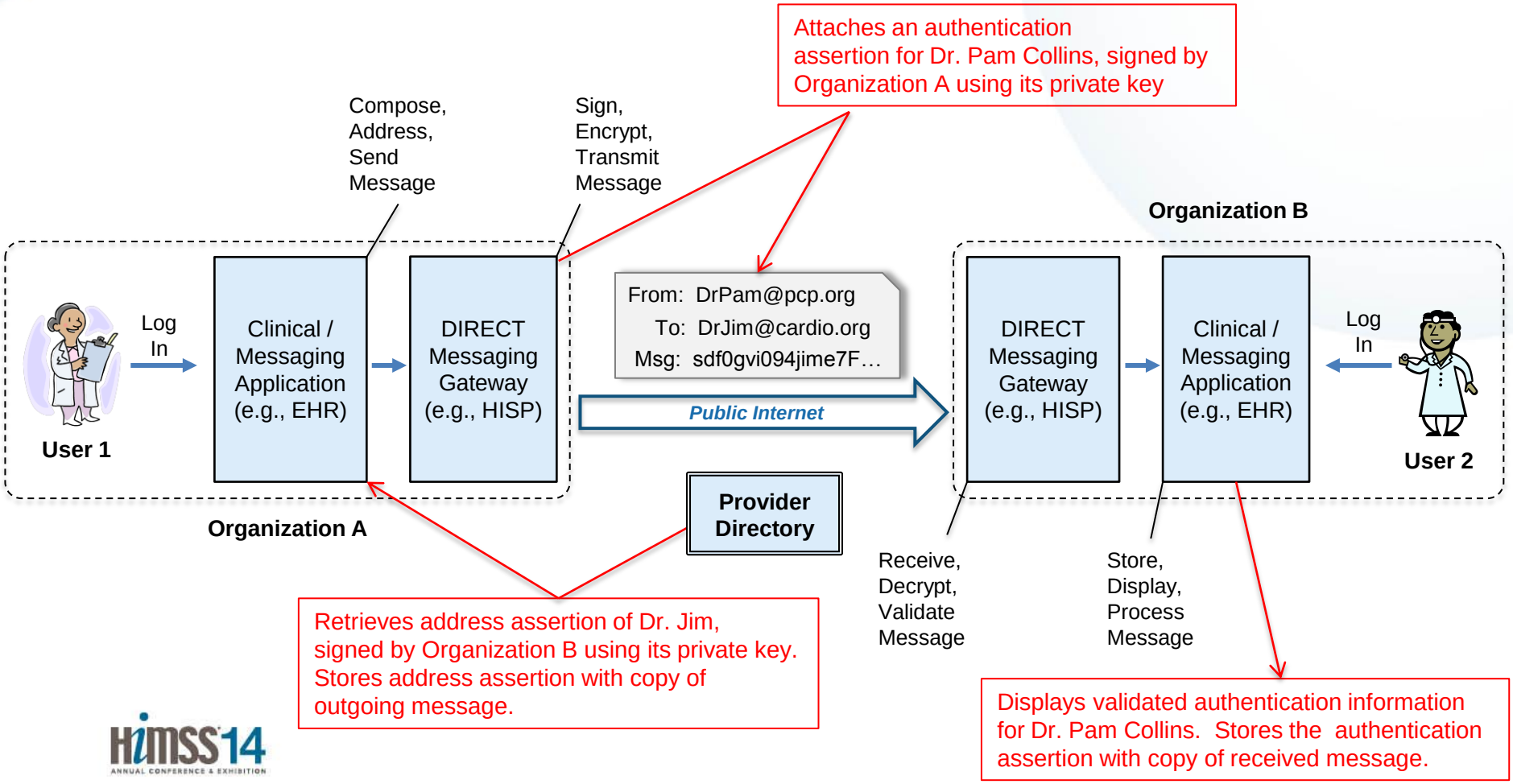
- XML data structure; industry standard (OASIS)
- Extensible data model for specific use cases
  - Authentication assertion (e.g., includes method of authentication)
  - Address assertion (e.g., includes DIRECT address, supported transactions)
- May be digitally signed by the issuing entity
- Example:

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer>pcp.org</saml:Issuer>
  <saml:AuthnContextClassRef>Password</saml:AuthnContextClassRef>
  <saml:AttributeStatement>
    <saml:Attribute Name="FullName">Pamela Collins</saml:Attribute>
    <saml:Attribute Name="NPI">5784798773</saml:Attribute>
  </saml:AttributeStatement>
  <saml:Signature>AzID5hhJeJlG2llUDvZswNUrlrPtR7S37Q...</saml:Signature>
  <saml:X509Certificate>MIIEATCCAumgAwIBAgIBBTANBgkq...</saml:X509Certificate >
</saml:Assertion>
```

Approaches to Establishing Trust: A Supplemental Model

- Operational Constructs:
  - Digital certificates created for covered entities by trusted CAs, following a rigorous identity-proofing process
  - Private keys are securely delivered to covered entities
  - Covered entities are responsible for maintaining the security of their private keys (and revoking associated certificates if keys are compromised)
  - Authentication assertions are included as attachments to each DIRECT message
    - May be archived by the recipient of the message for forensic purposes
  - Address assertions are published in provider directories
    - May be archived by the senders of outgoing messages for forensic purposes

DIRECT Messaging for Health Information Exchange



HIMSS14 ANNUAL CONFERENCE & EXHIBITION

Benefits of the Supplemental Trust Model

- Clear Accountability
  - Responsibility for PHI in DIRECT messages falls directly and trace-ably upon specific covered entities and their contracted agents
  - Security responsibilities of covered entities based on familiar HIPAA Security and Privacy rules
  - Covered entities contractually bind agents to fulfill certain of their security responsibilities (HISPs, Provider Directories, EHRs, etc.)
- Flexibility
  - Covered entities may fulfill their security responsibilities in whatever ways they feel are appropriate to protect themselves against the risks and liabilities of improper PHI disclosure during DIRECT messaging
- Decentralization and Scalability
  - Certificate authorities are the only centralized entities that must be trusted by all senders and recipients of DIRECT messages

The Healthcare Benefits of a Decentralized and Scalable Trust Framework for DIRECT Messaging

- Secure exchange of patient health information as ubiquitously and conveniently as conventional email messaging
- Low-cost, low-overhead communication channel for many of the Stage-2 M.U. measures that require interoperability, including:
  - Transitions of care and referrals
  - Delivery of structured lab results
  - Submission of data to immunization registries
- Improved care coordination among all clinical settings, regardless of type, size, or business affiliation

Thank You!

Questions?

Walter Sujansky
Sujansky & Associates, LLC
walter@sujansky.com

Sujansky & Associates LLC

HIMSS14 ANNUAL CONFERENCE & EXHIBITION