EHNAC

Electronic Healthcare Network Accreditation Commission

A Closer Look at Securing the Data Exchange Models of HIE/HIO/ACO and the Direct Protocol

June 17, 2015

Presented by Lee Barrett, Executive Director

www.ehnac.org

HIMSS NEW YORK STATE Chapter

Agenda

- Healthcare's Exchange Structure Overview
- The Office of the National Coordinator for Health Information Technology's (ONC's) Push to Advance Nationwide Health Information Exchange
- Stronger Direct Connections: Direct Project
- Accrediting Those Connections: The EHNAC Factor
- Collaboration between DirectTrust and EHNAC: DTAAP

Today's Objectives

- Explore the healthcare industry's existing efforts to assure interoperability and scalable trust;
- Understand the ONC's role in achieving stakeholder adoption;
- Evaluate the industry drivers around clinical exchange, securing messaging and authentication = The Direct Project;
- Explain the significant differences between EHR technology software certification and security/trust accreditation for HISPs, CAs and RAs who partner with EHRs;

Today's Objectives *continued*

- Provide best practice examples of how to facilitate security, interoperability and trust among exchange participants, fostering public confidence, and promoting the adoption and success of all exchange stakeholders; and
- Describe ways to reduce PHI exposure risks through the demonstration of comprehensive risk management programs.

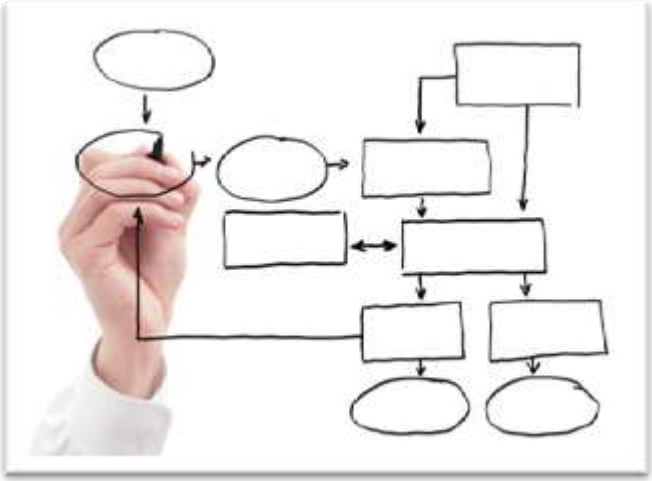
HEALTHCARE'S EXCHANGE STRUCTURE OVERVIEW

Health Information Exchange (HIE) Market Reality

- HIE facilitated by a variety of organizations/sources including:
  - HIOs
  - HISPs
  - EHR vendors
  - National services providers
  - Hospitals
  - ACOs
  - Health Center Controlled Networks
  - Others

Health Information Exchange Truths

- Health information exchange is a journey, not a destination
- Leveraging government parameters can support conditions of exchange
- Health information exchange is not one-size-fits-all
- Multiple approaches will exist side-by-side
- Build in incremental steps – "don't let the perfect be the enemy of the good"



Evolving Compliance Issues Affecting HIEs and ACOs

- The advent of the HITECH Omnibus Rule
  - Additional compliance provisions that place increased penalties for PHI disclosures and breaches
- The Office for Civil Rights (OCR) have been reinstituting OCR audits in earnest
  - OCR conducted 115 audits in 2012 with a cross section of healthcare stakeholders
- EHNAC has worked for the past year with OCR to further align accreditation programs with OCR audit protocol

THE ONC'S PUSH TO ADVANCE NATIONWIDE HEALTH INFORMATION EXCHANGE

ONC Strategies to Advance Nationwide Exchange

- Enable a governance infrastructure, including a trust framework, that reduces barriers to exchange;
- Coordinate across federal government partners on HIE funding, innovations and implementations;
- Create shared learning opportunities to identify best practices and lessons learned to advance exchange;
- Help vendor community (HER. PMS,HIE, ACO…) understand meaningful use requirements and options;

Connecting America for Better Health
The Office of the National Coordinator for Health Information Technology

ONC's Strategies to Advance Nationwide Exchange, *continued*

- Support state-level and community HIT-enabled care transformation; and
- Convene state policy leaders, federal partners and other leaders to tackle and resolve specific issues confronting on the ground implementers who are using HIT to support state-level care transformation including quality reporting, analytics, care coordination and patient engagement.

Reduce Cost and Increase Trust and Value

COST

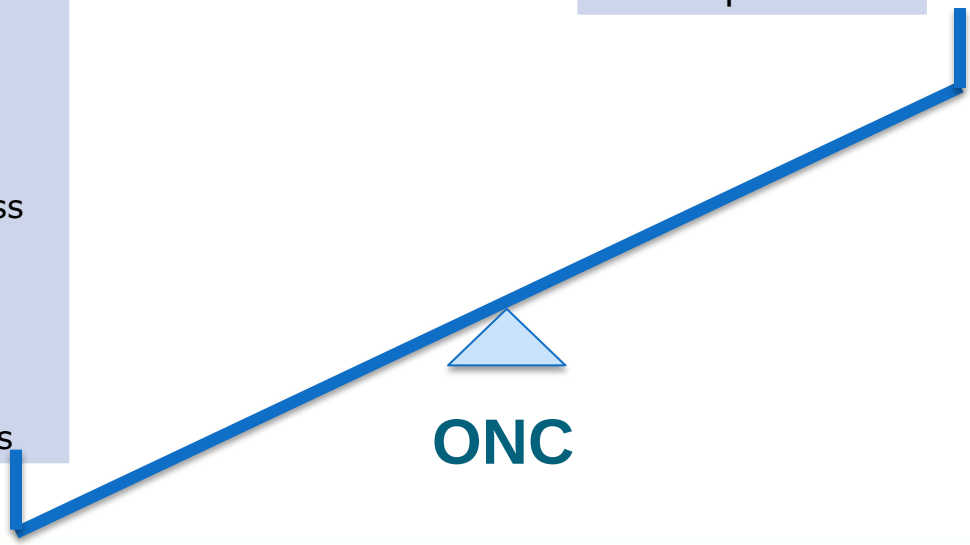
Standards: identify and urge adoption of scalable, highly adoptable standards that solve core interoperability issues for full portfolio of exchange options
Market: Encourage business practices and policies that allow information to follow patients to support patient care
HIE Program: Jump start needed services and policies

VALUE

- Payment reforms
- Meaningful Use
- Wide-scale adoption

TRUST

- Identify and urge adoption of policies needed for trusted information exchange



STRONGER DIRECT CONNECTIONS:

THE DIRECT PROJECT

What is the Direct Project?

- The Direct Project seeks to benefit patients and providers by improving the transport of health information, making it faster, more secure, and less expensive. The Direct Project will facilitate "direct" communication patterns with an eye toward approaching more advanced levels of interoperability than simple paper can provide.

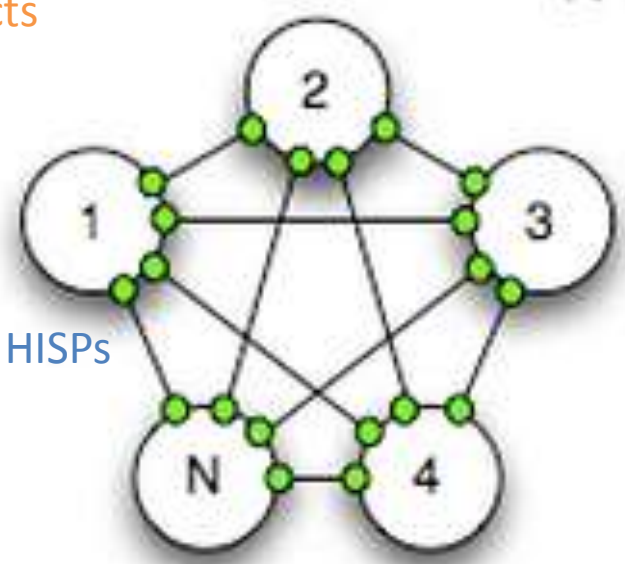
The Direct Project specifies a *simple, secure, scalable, standards-based* way for participants to send authenticated, encrypted health information *directly* to *known, trusted recipients over the Internet.*

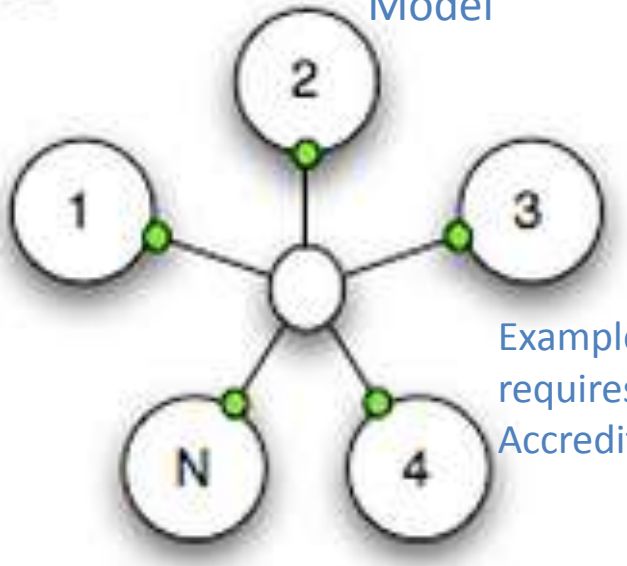
The n(n-1) Connection Problem, Also Known as the N Squared Problem

Bi-directional Contracts Model

N Squared

Single Accreditation Model





Example: 8 HISPs requires 28 Contracts {N(n-1)/2}

Example: 8 HISPs requires 8 Accreditations

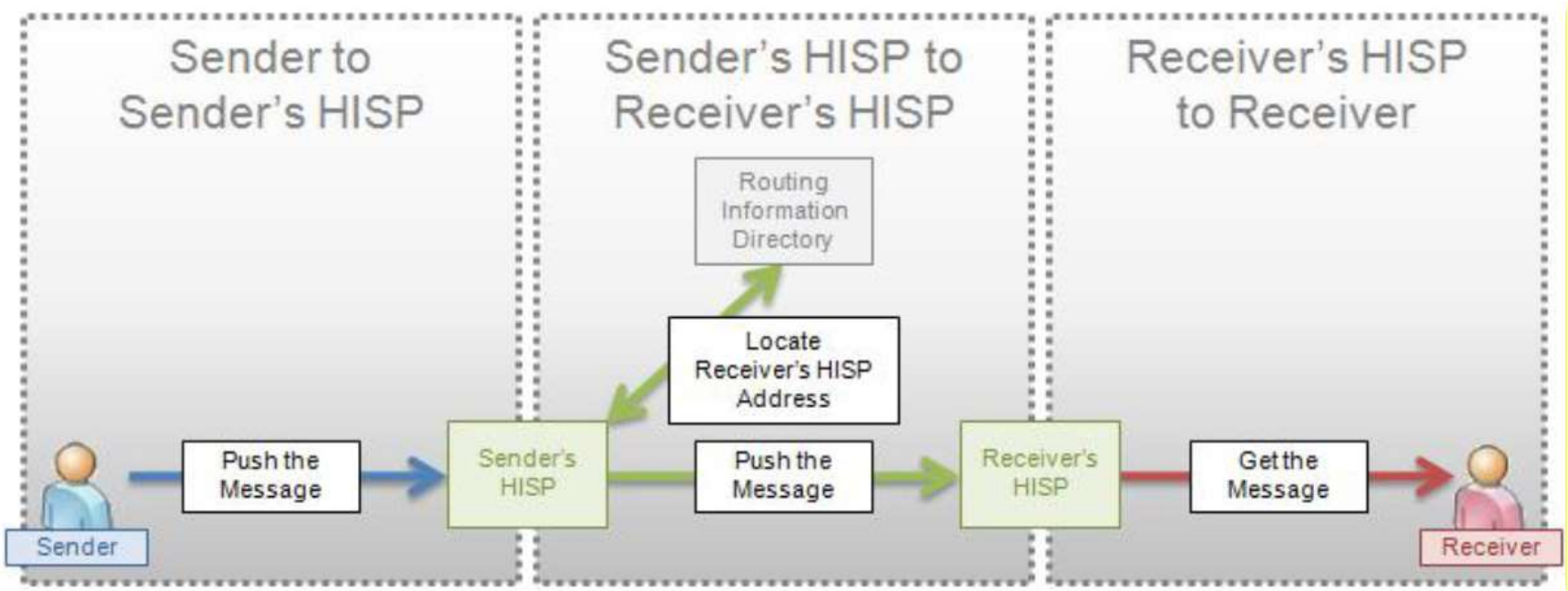
When N is large, # Interfaces $\sim N^2$

Interfaces = N

Each 2 interfaces requires a contract

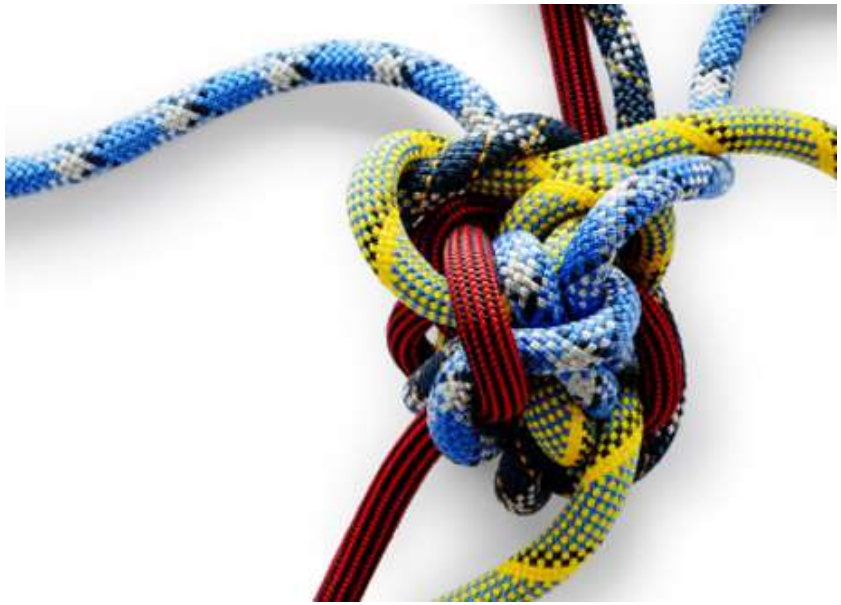
Direct Technology Facilitates Seamless Transitions of Care

Direct Abstract Model



Building Network Via Bi-directional Contracts Is Unworkable

- If HISPs have to forge one-off contracts with each other, the cost of Directed exchange goes UP with each new user group, each new contract, and thus the value decreases. Complex. Rate-limiting step.



Key Issues for Scalable Trust: Identity and Security

- Directed exchange is email over the Internet.
- Sender and receiver depend on one another for identity validation and encryption of message and attachments.
- Without trust in these, inability to establish service connections between HISPs are likely, leading to service interruptions.
- Roles for “trusted agents” – who supply identity validation and encryption – are critical, because they are potential weak links in the network of trust.
- What constitutes sufficient trust and how can we avoid costly, time consuming contracts between each HISP? That is, how can trust become scalable?

Scalable Trust

- Scalable Trust is a strategy for enabling Directed exchange between a large number of endpoints, in this case HISPs and their users/subscribers.
- If “scalable,”
  - Trust should happen “quickly” and uniformly.
  - A “complete” network will be formed voluntarily.
  - Complexity and cost of establishing a network will decrease, while the value of the network itself will increase, as more nodes are added.
  - This “network effect” will be a by-product of making trust scalable.

"Before DirectTrust.org, no one knew I was a dog."

ACCREDITING THOSE CONNECTIONS: THE EHNAC FACTOR

EHNAC History/Governance

- Founded in 1995 as an independent, 501(c)(6) not-for-profit accreditation organization
- Federally recognized as a standards development organization (SDO)
- 70+ accredited organizations
- Legislated in the states of MD and NJ w/ others considering specific accreditation program adoption
- Governed by a Commission of 14 industry stakeholders from private and public sector organizations
- Guided by peer evaluation promoting quality service, innovation, cooperation and open competition

EHNAC's Mission

- Improve the transactional quality, operational efficiency and data security of protected health information;
- Assist industry stakeholders in achieving compliance with healthcare legislative mandates including HIPAA, ARRA/HITECH, Affordable Care Act, and the recent Omnibus Rule, as well as regulatory guidelines; and
- Promote standards-based accreditation within the healthcare data exchange industry to improve the quality of care delivery.

EHNAC's Strategies

- Develop standard criteria and accredit organizations that electronically exchange healthcare data
- Provide accreditation services for:
  - Electronic Health Networks (EHNs)/clearinghouses
  - Financial Services Organizations
  - Payers and Third-Party Administrators (TPAs)
  - E-prescribing Networks
  - Health Information Service Providers (HISPs), Certificate Authorities (CAs), and Registration Authorities (RAs)
  - Health Information Exchanges (HIEs)
  - Accountable Care Organizations (ACOs)
  - Managed Service Organizations (MSOs)
  - Medical Billers
  - Other healthcare industry organizations

Criteria Development

Development

- Criteria Committee recommends new and modified criteria to Commission
- Commission Approves, Rejects, or sends back to Criteria Committee

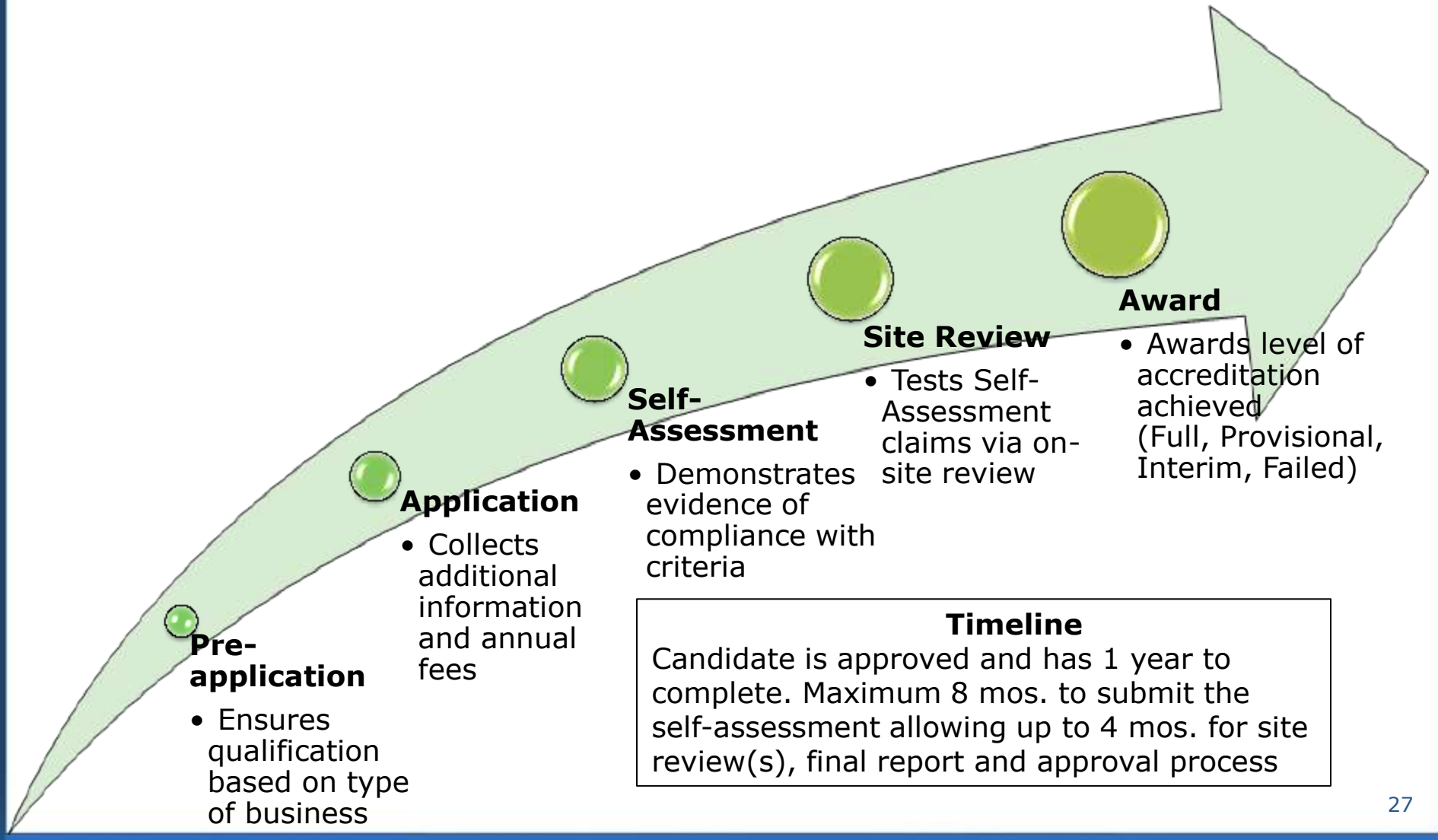
Criteria released for public comment, with press release

Comment period of at least 60 calendar days

Final modifications per comment period

Executive Committee recommends final revision to Commission

EHNAC Accreditation Process



Timeline

Candidate is approved and has 1 year to complete. Maximum 8 mos. to submit the self-assessment allowing up to 4 mos. for site review(s), final report and approval process

Benefits of Accreditation

- General Benefits
  - Provides a competitive advantage and differentiation
  - Showcases compliance with EHNAC criteria
- Framework
  - Provides a framework for reusable policies and procedures
  - Promotes industry best practices in healthcare
  - Identifies areas for improving business processes/workflows
  - Facilitates business discipline, organization and planning
- Metrics
  - Enhances performance through requirements for quality metrics and measurements
  - Improves customer satisfaction through the capture of call metrics

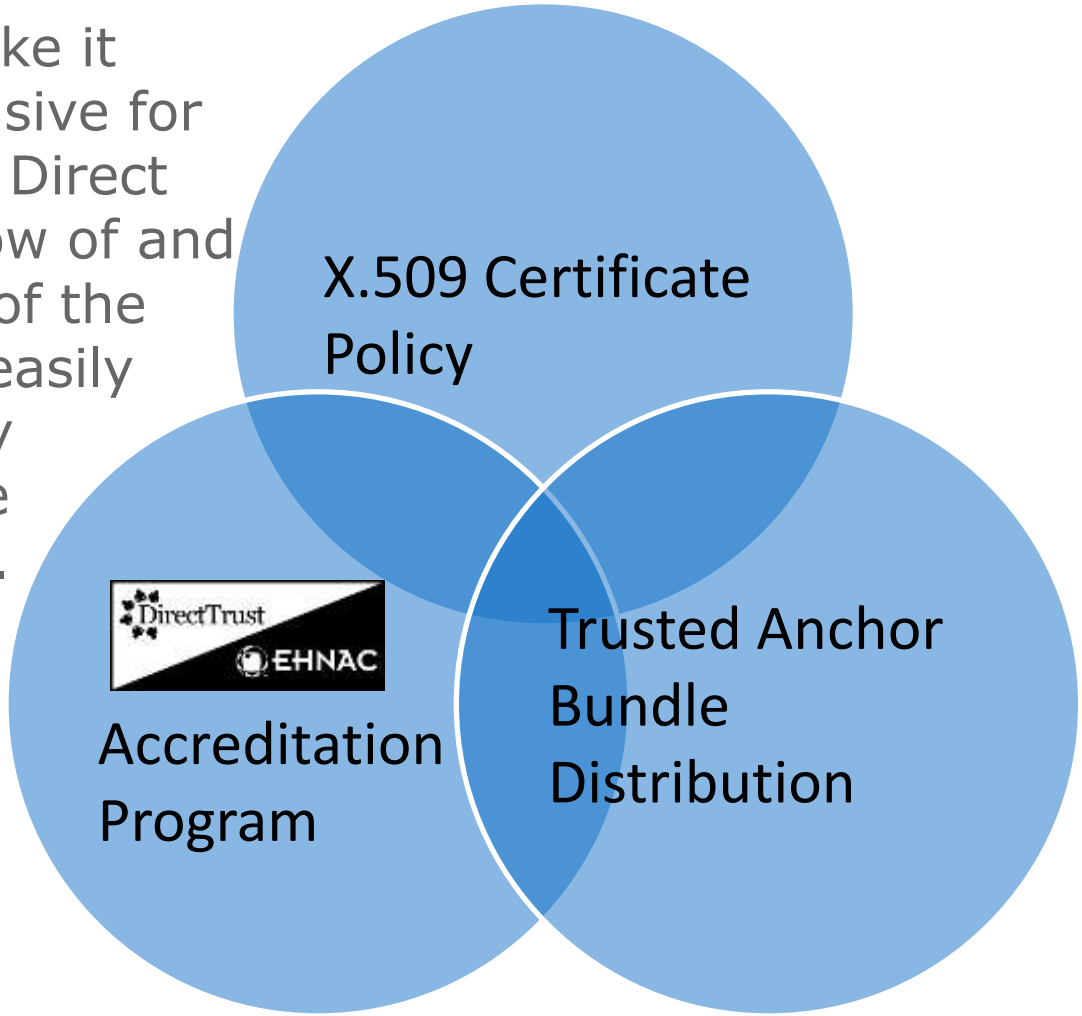
Benefits of Accreditation, *continued*

- Quality
  - Encourages quality improvements in products and services
  - Fosters operating cost reductions through efficiencies
  - Provides regular, comprehensive and objective evaluation of policies, procedures and controls
- Compliance
  - Reviews HIPAA, ARRA/HITECH, Affordable Healthcare Act, Omnibus Rule and other regulatory compliance requirements
  - Alliance with OCR Audit Protocol
  - Fulfills Maryland, New Jersey and Texas regulatory requirements
  - Identifies privacy, security, confidentiality and business risk exposures and mitigation strategies

COLLABORATION BETWEEN DIRECTTRUST AND EHNAC: DIRECT TRUST AGENT ACCREDITATION PROGRAM (DTAAP)

DirectTrust Framework

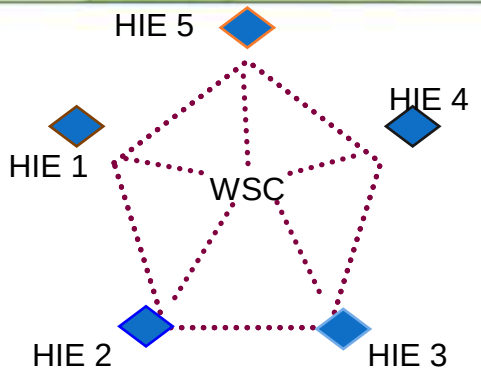
The goal is to make it easy and inexpensive for trusted agents in Direct to voluntarily know of and follow the "rules of the road" while also easily and inexpensively knowing who else is following them.

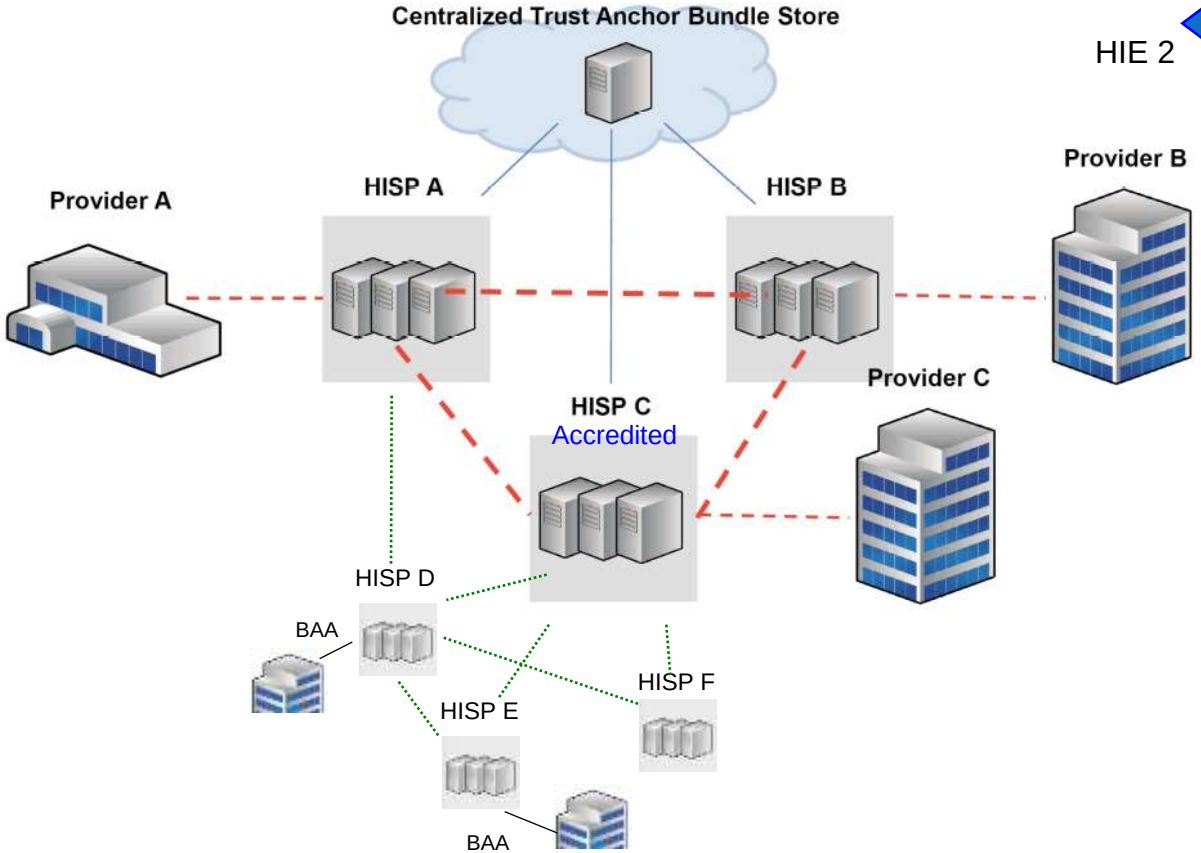


The Real World

Key

- Trust relationship based on accreditation
- Trust relationship based on participation agreement
- Trust relationship based on bi-directional contract



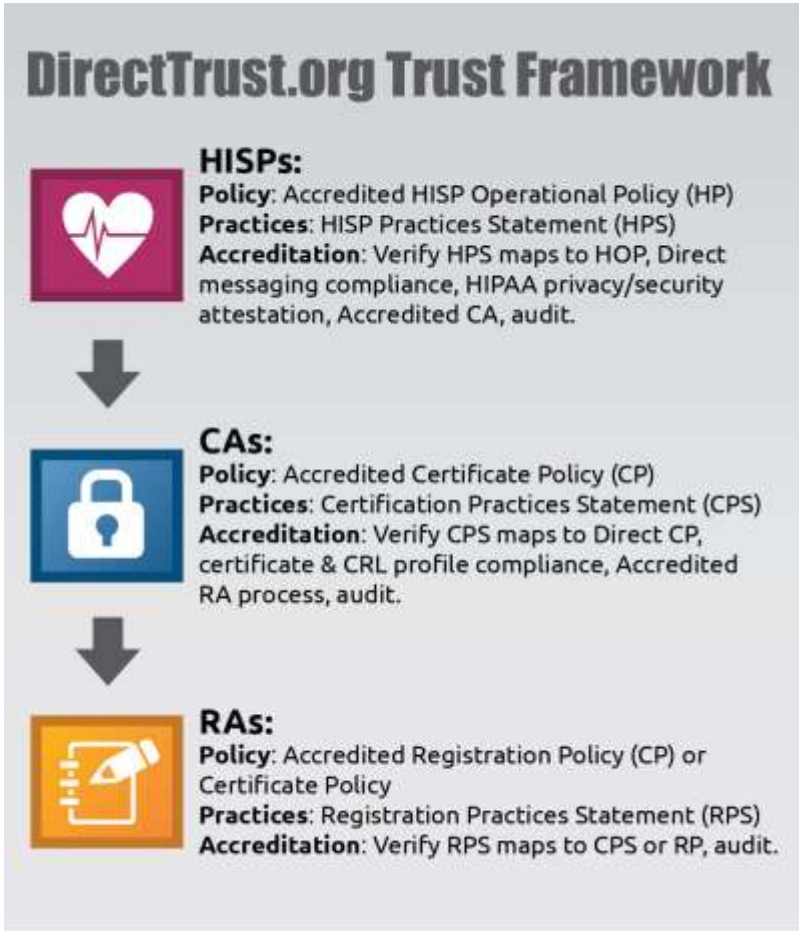


Direct Trusted Agent Accreditation Program

- The "stamp of approval" from industry peers recognizing excellence in health information technology and transactions
- Assesses compliance with industry-established standards in
  - privacy and confidentiality
  - technical performance
  - business practices
  - resources
  - security
- Reviews HIPAA privacy and security requirements

Accrediting Trusted Roles

- The DTAAP provides a baseline set of standards for the management and operations of HISPs, CAs, and RAs within the DirectTrust Framework.
- Accredited entities can be trusted by relying parties within the Direct community to be:
  - operating in accordance with the collective policies and processes proscribed by DirectTrust
  - subject to annual audits



DTAAP Structure

Contents

SECTION I: INTRODUCTION TO CANDIDATE ENVIRONMENT FOR HISP, CA, AND RA 6

SECTION II: PRIVACY AND CONFIDENTIALITY FOR HISP, CA, AND RA 7

SECTION III: GENERAL SECURITY PROFILE SPECIFICATIONS FOR HISP, CA, RA 9

SECTION IV: IMPLEMENTATION SPECIFICATIONS FOR HISP 10

SECTION V: IMPLEMENTATION SPECIFICATIONS FOR CA 12

SECTION VI: IMPLEMENTATION SPECIFICATIONS FOR RA 15

SECTION VII: TECHNICAL PERFORMANCE FOR HISP, CA, AND RA 18

SECTION VIII: BUSINESS PRACTICES FOR HISP, CA, AND RA 20

SECTION IX: RESOURCES FOR HISP, CA, AND RA 21

SECTION X: SECURITY FOR HISP, CA, AND RA 22

DTAAP Criteria Examples

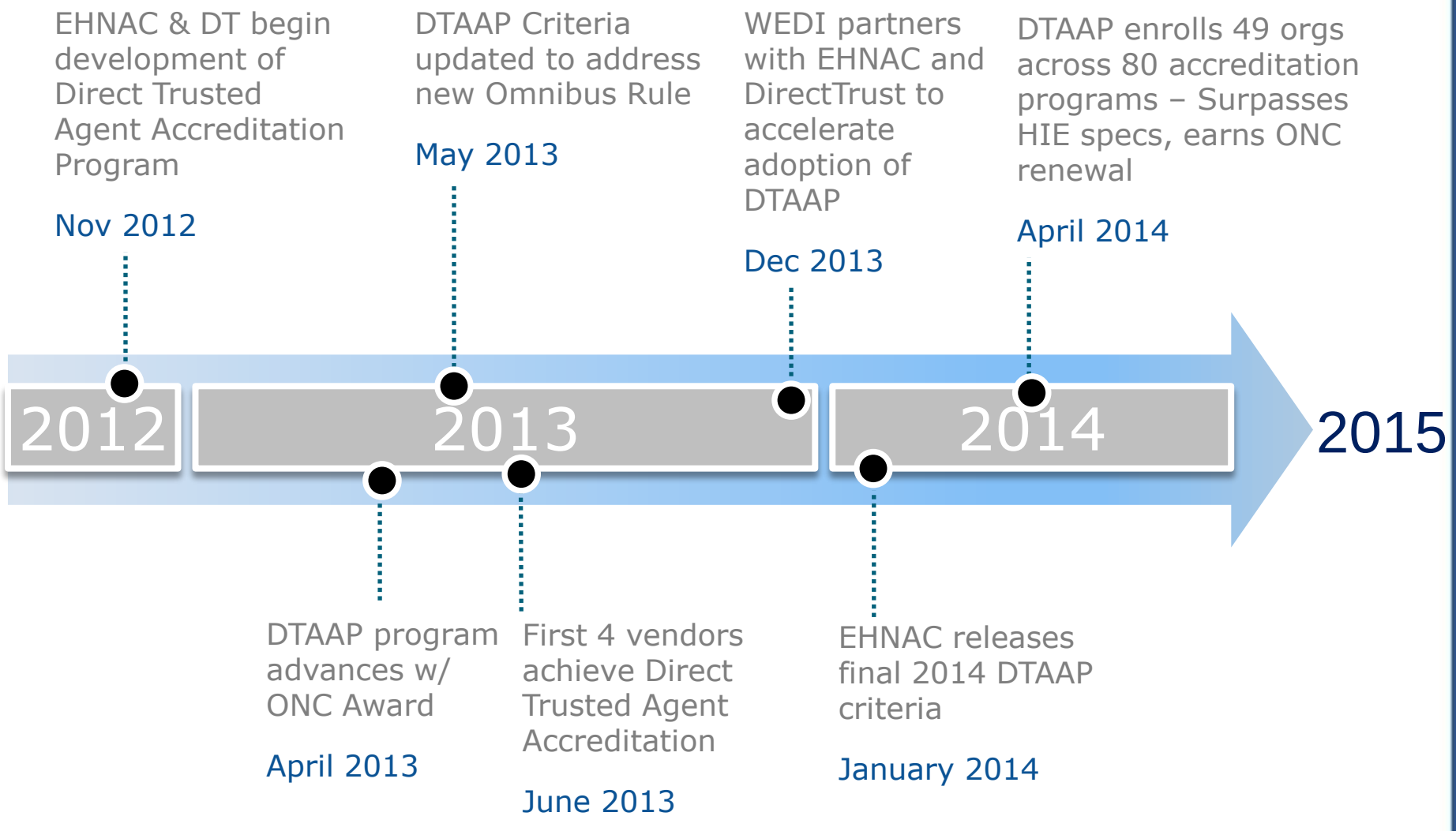
II.A.8 **[MANDATORY]** (G) Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on personal computers, consumer devices, and removable storage media.
{410} 45 CFR §§ 164.530(c)

IV.A.2 **[MANDATORY]** (H) Candidate's HISP Services must support DNS and LDAP methods for discovering recipient certificates as specified in the S&I Framework Certificate Discovery for Direct implementation Guide.
{DTAAP-0004}

V.A.8 **[MANDATORY]** (C) Candidate's Distinguished Name (DN) must be linked to one and only one Direct Entity (DE) over the lifetime of the Certificate Authority.
{DTAAP-0026}

VI.B.7 **[MANDATORY]** (R) Candidate's RA Services must record and retain all requests and responses for identity verification activities, even when or after this information is passed to the appropriate CA.
{DTAAP-0052}

DTAAP Timeline



Questions?

Lee Barrett

Executive Director

EHNAC

lbarrett@ehnac.org

860.408.1620