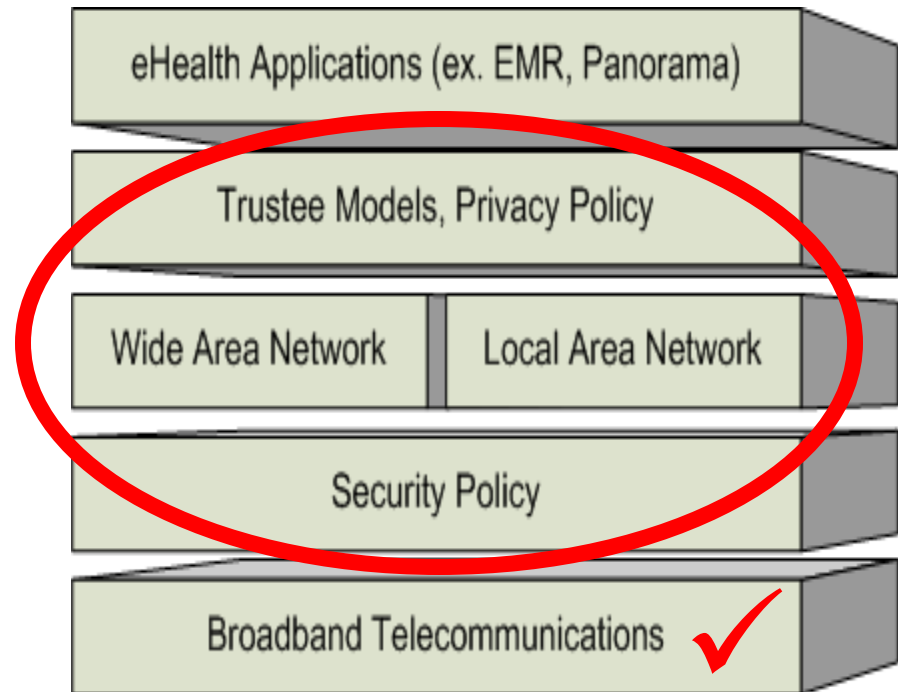# *Readying the NITHA Communities for Integrated eHealth*
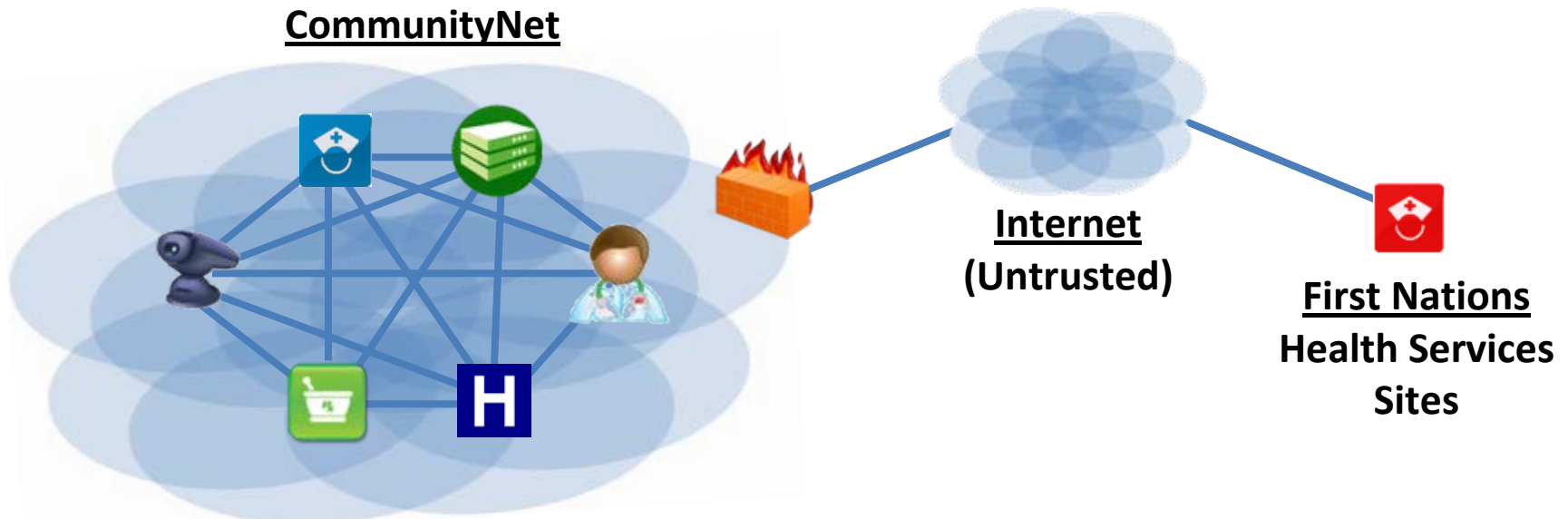
Objectives

1. Implement a Privacy Program and Establish a Data Trustee Model

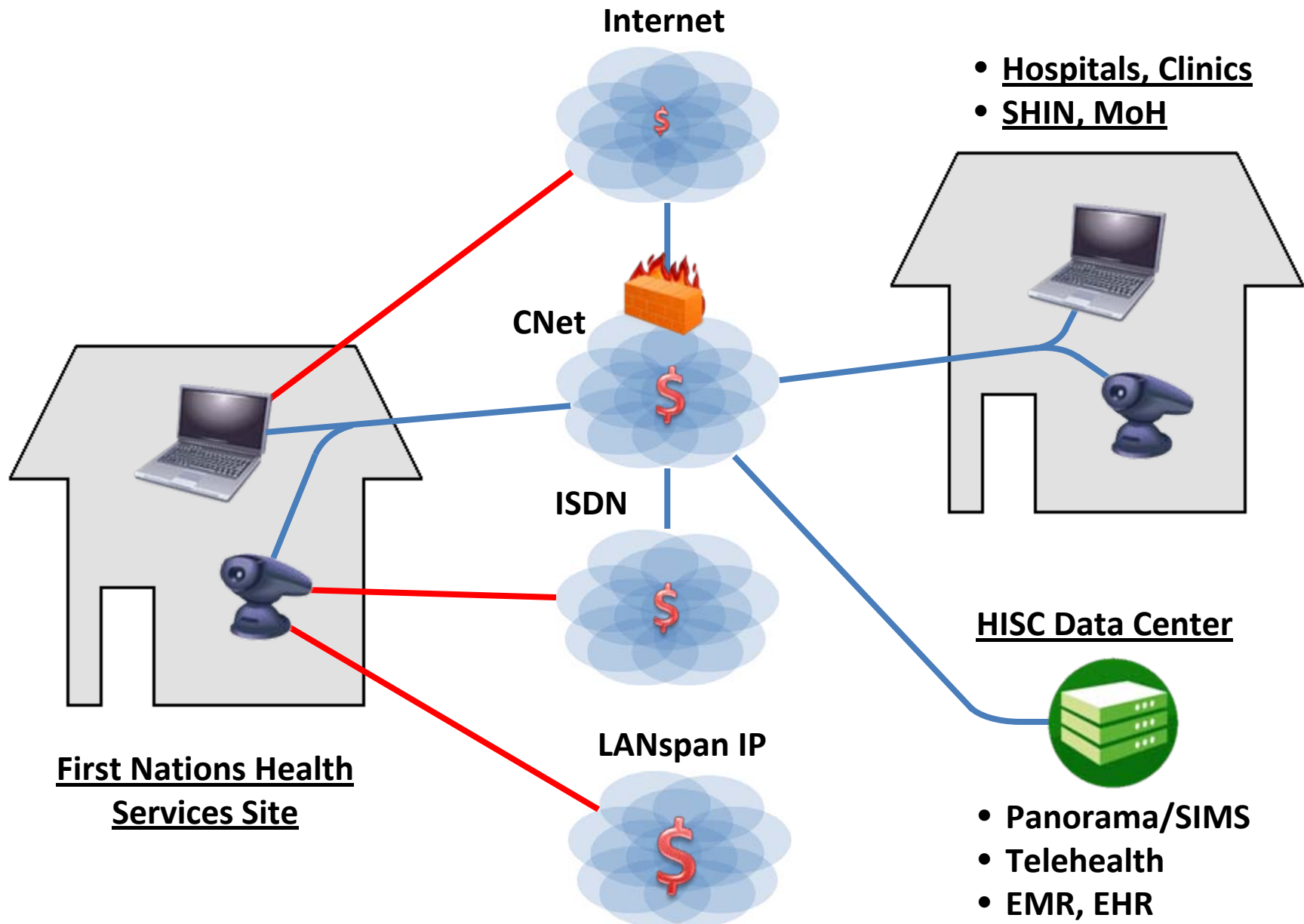2. Migrate First Nations to the Provincial Electronic Health Network (a.k.a. CommunityNet)

CommunityNet

What is CommunityNet?

- CommunityNet is a *Secured Private* Electronic Network connecting Provincial Hospitals, Pharmacies, Clinics, Physicians Offices, etc.

- First Nations Health were not part of the original CommunityNet Initiative

CommunityNet

Internet
(Untrusted)

First Nations
Health Services
Sites

Why CommunityNet?

Internet

- **Hospitals, Clinics**
- **SHIN, MoH**

CNet

ISDN

HISC Data Center

LANspan IP

First Nations Health Services Site
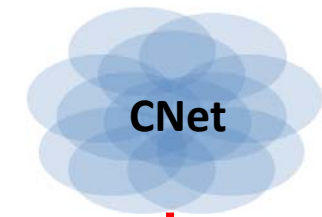
- **Panorama/SIMS**
- **Telehealth**
- **EMR, EHR**

Preparing & Standardizing the Health Facilities for CommunityNet

Network Hub: Enclosed Rack Patch Panel, UPS, CNet CPE, Cisco ASA, Cisco Switches

CNet

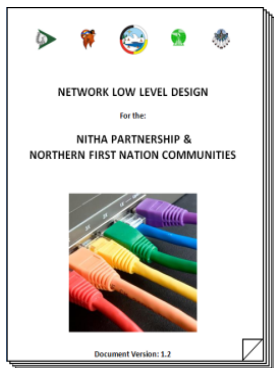**Install CommunityNet Services**

Cat5/6 Cabling

Wireless Access Points

- **High & Low Level Design and Configuration/Procedural Document**
- **Cisco Training for IT Personnel**

CommunityNet Outputs

- Increased Network Security
- Lower Telecommunications Costs
- Better Network Performance
- Easier Network Management

CommunityNet Outcomes

- Network Standardization
- Interoperability with Province

Challenges

Challenge	Addressing the Challenge
• Not Enough IT Personnel (HR)	• Dedicating Existing Personnel's time • Partner Investment
• Not Enough Funding	• Partner Investment

Privacy & Security

Specific Objectives

- To improve the Privacy & Security Practices within First Nations Health Services in order to protect the Confidentiality of Sensitive [Health] Information in an Integrated environment

- To take formal Ownership & Control of First Nations Data by establishing First Nations as "Trustees" and prepare for *"Data Sharing"* with other Trustees for better Health Outcomes

Definitions

PRIVACY is the inherent right of individuals to have their personal [health] information protected during its collection, use, discloser and disposal

SECURITY are precautionary measures to protect the confidentiality, integrity and availability of information

CONFIDENTIALITY is the obligation to respect and protect information.

Definitions

TRUSTEES are organizations or individuals that have custody or control of Health Information and are responsible for the protection of that information

TRUSTEE MODELS are structures for ensuring health information is protected among Trustees.

DATA SHARING AGREEMENTS spell out what information is shared among Trustees, for what purpose, limiting use, etc.

Building a Privacy & Security Program

Technical Safeguards

•*Passwords, Anti-Virus software*
•*Firewalls on computers*
•*Data Encryption*

Awareness and Training

•*Posters, Handbooks*
•*Presentations*
• *Workshops*

Physical Safeguards

• *Locks on file cabinets*
• *Restricted physical access*
• *Location of fax, printers*

Administrative Safeguards

• *Privacy & Confidentially*
• *Collection, Use, Disclosure,*
• *Reporting Breaches ?*

Organizational Roles

• *Health Directors, CEO, MHO,*
• *Health Care Professionals*
• *Staff/HR, [Designated] Privacy Officers*

Policy Development

Privacy Policies

- Definitions
- Access
- Confidentiality
- Collection
- Amendment
- Reporting Breaches
- Disposal
- Security and Storage
- Disclosure of PHI to Police
- Protection during use and disclosure
- Right to be informed

Security Policies

- Organization of Information Security
- Acceptable use of Technology
- Electronic Information Access Control
- Including Security in Job responsibilities
- Information Assets
- Password Management
- Reporting Information Security Incidents
- User Responsibilities

Implementing a [Interim] Trustee Model for (e)*Public Health* in the North
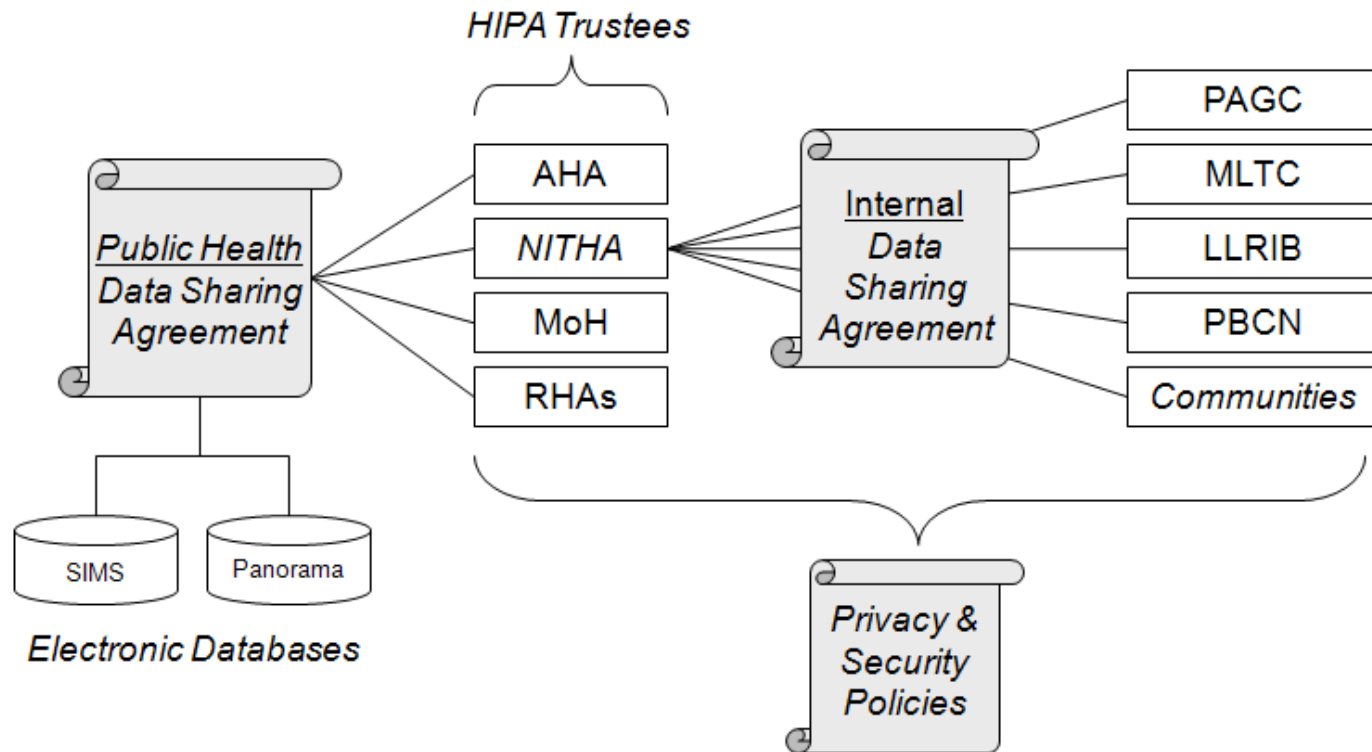
NOTE – there will be different trustees and trustee models for different information systems (ex. EMR, PIPS)

Key Activities

- Staffed a Privacy Officer to facilitate the Privacy & Security Capacity Development within the NITHA Partnership

- Setting up Privacy Working Groups
  - Develop a Training & Awareness program
  - Review, Revise, and Recommend Policies, Procedures, Material, Training and Awareness Processes, and dissemination

Privacy & Security

Challenge	Addressing the Challenge
• Availability of Individuals	• Work around the availabilities of individuals
• Levels of Authority	• Communicate Issues to Leadership
• Fear and Mistrust	• Education & Awareness • Correlate OCAP with established Processes

Thank You