ROME

EUROPEAN TELEMEDICINE CONFERENCE

7-8 OCTOBER 2014 | ROME, ITALY

# IMPROVING SECURITY THROUGH STANDARDS

BRIDGET A. MOORMAN, CCE, CONSULTANT
MHEALTH COMPETENCE CENTRE OF MOBILE WORLD CAPITAL BARCELONA

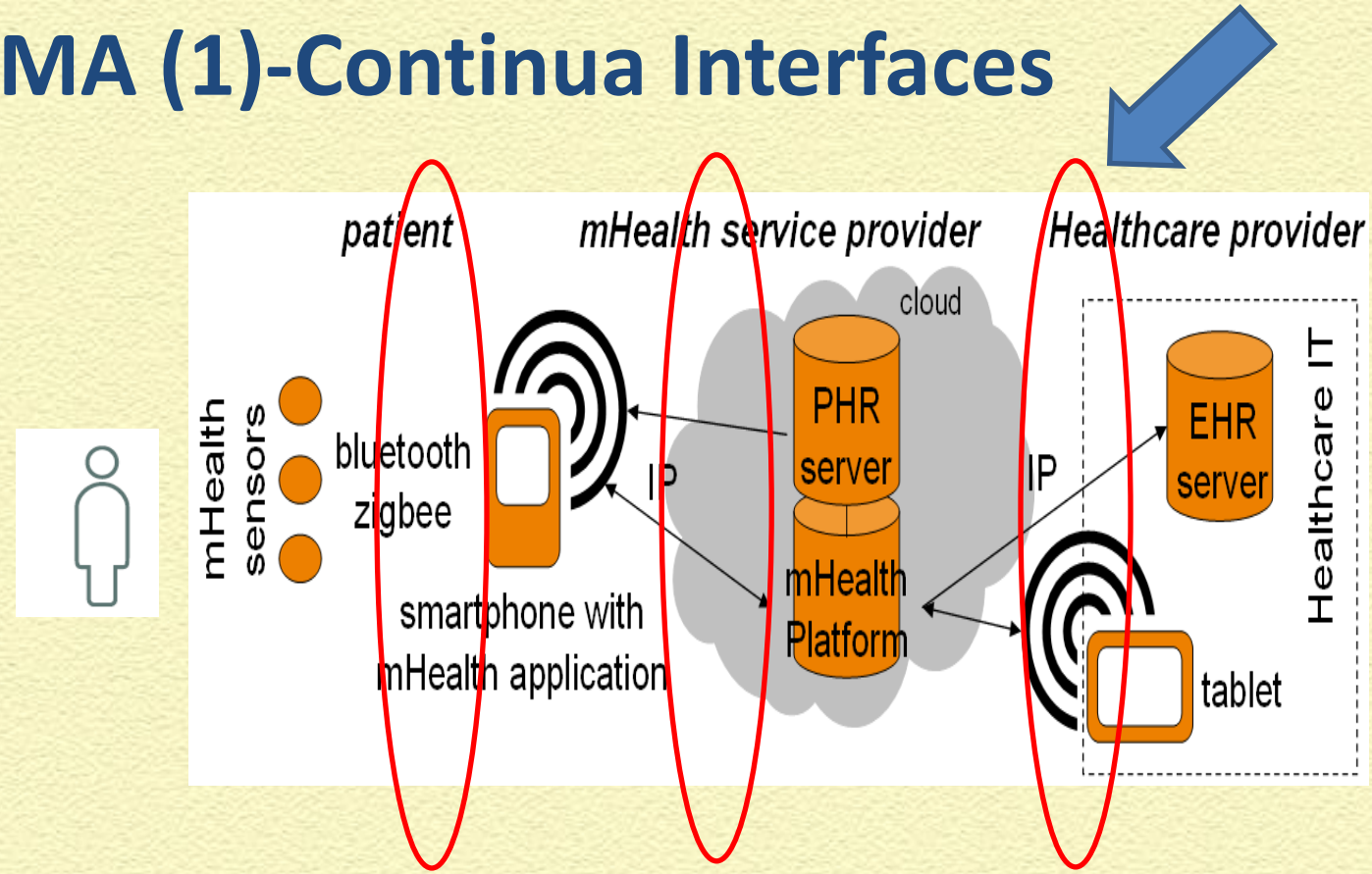
# Overview

- 5 A's of Security
- Sample Mobile Telehealth Architecture
- Continua Guidelines – Security
- mHIMSS Privacy and Security Recommendations
- What is Being Done? (Norway example)
- Summary

# Five A's of Security-b ISO 27000

- Authorization
  - Only those authorized should have access – Identification, Confidentiality, Integrity, and Authenticity
- Accountability
  - Users should be accountable for their actions – non-repudiation
- Availability
  - System should be available for use when required
- Administration
  - Security Policy should be easily administered
- Assurance
  - Claimed level of protection should be prove-able

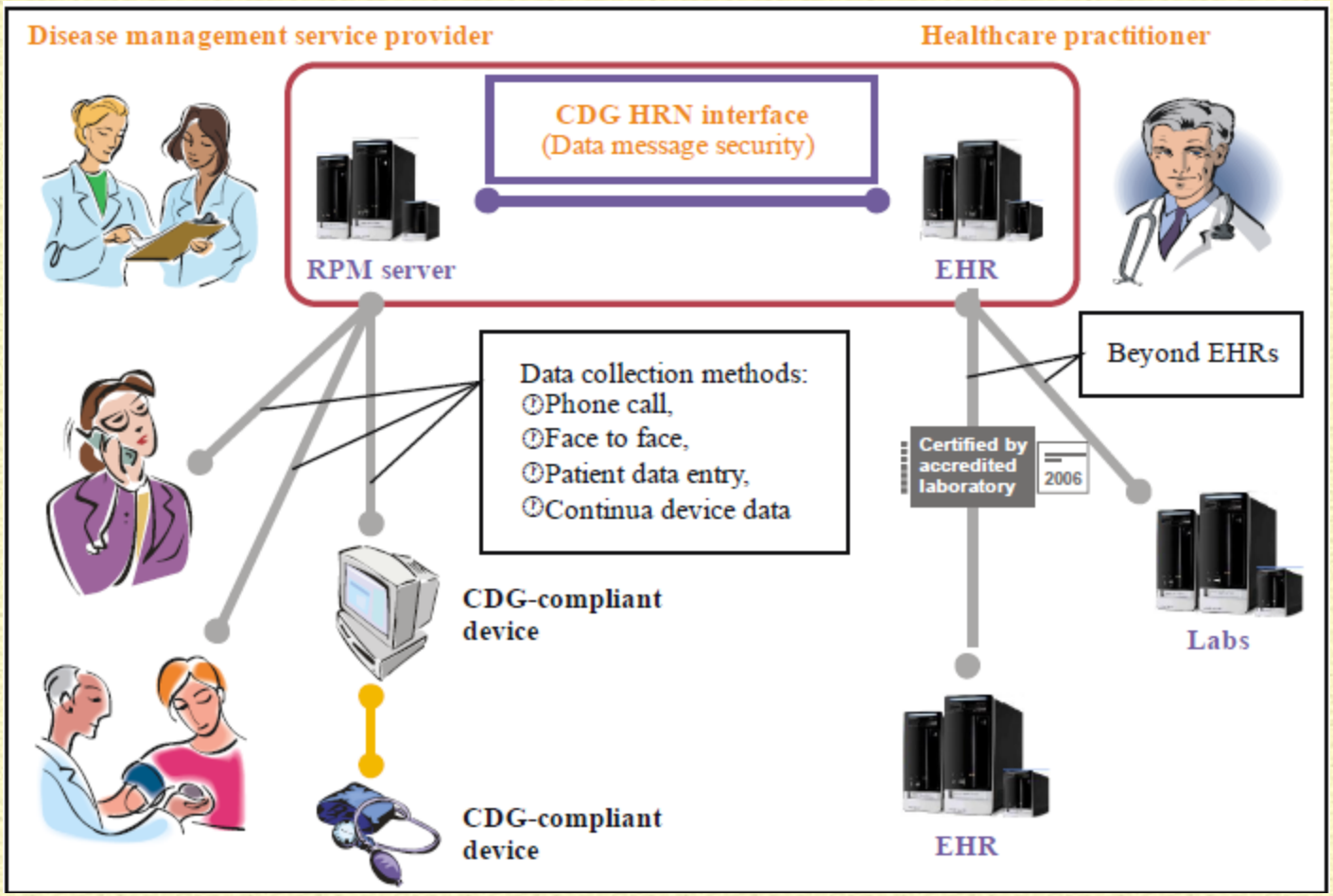
# Sample Mobile Telehealth Architecture- GSMA (1)-Continua Interfaces



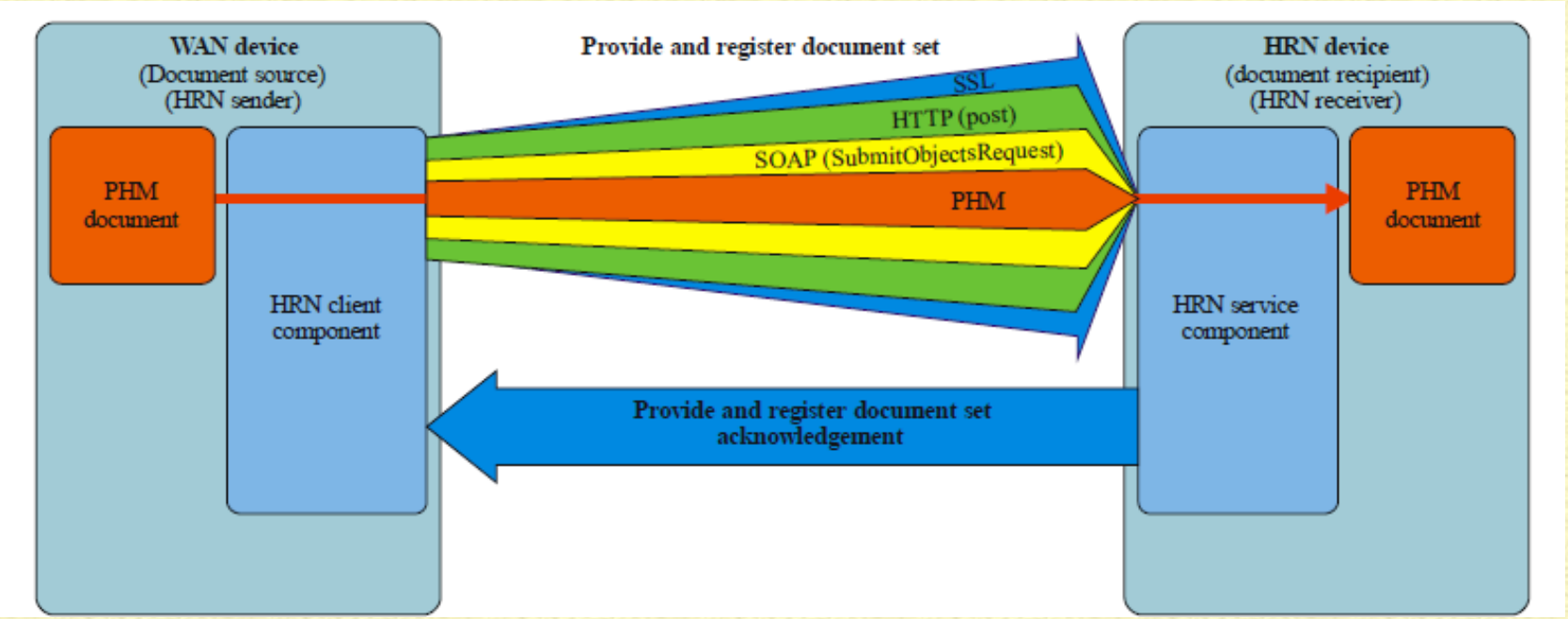

CONTINUA I/F'S PAN/TAN/LAN WAN HRN and/or WAN

1) Moorman, B, with R. Cockle, "Medical Device Integration Using Mobile Telecommunications Infrastructure", Biomedical Instrumentation and Technology, May/June 2013, Vol. 47, No. 3, pp. 224-232

# Continua HRN Scope-General Use Case



# Continua Depiction of HRN Direct via XDR Transaction




Uses VPN SSL, web based secure connection, which is administered at OSI layers 4.5, versus VPN IP Sec, which is administered at OSI layer 3

# Continua Guidelines 2014-Security

| INTERFACE | SECURITY PRINCIPLE | STANDARD |
|---|---|---|
| PAN/LAN | Authorization (Confidentiality, integrity, authentication) | BlueTooth/ZigBee Security |
| WAN | Authorization (confidentiality, integrity and service/entity authentication) | WSI BSP (TLS 1.0 and WS-Security + SAML 2.0) |
| HRN | Authorization (confidentiality, integrity, authentication) and Accountability (non-repudiation) | TLS V1.0 (IETF RFC 2246); IHE XDM; IHE TF-1 XDS XUA; IHE ITI TFS DSG |
| HRN | Administration; identify management | IHE ITI 44, 45, 47 (IHE ITI PIX PDQ) |
| WAN, HRN | Administration (Auditing) | IHE ATNA (IETF RFC 3881) |

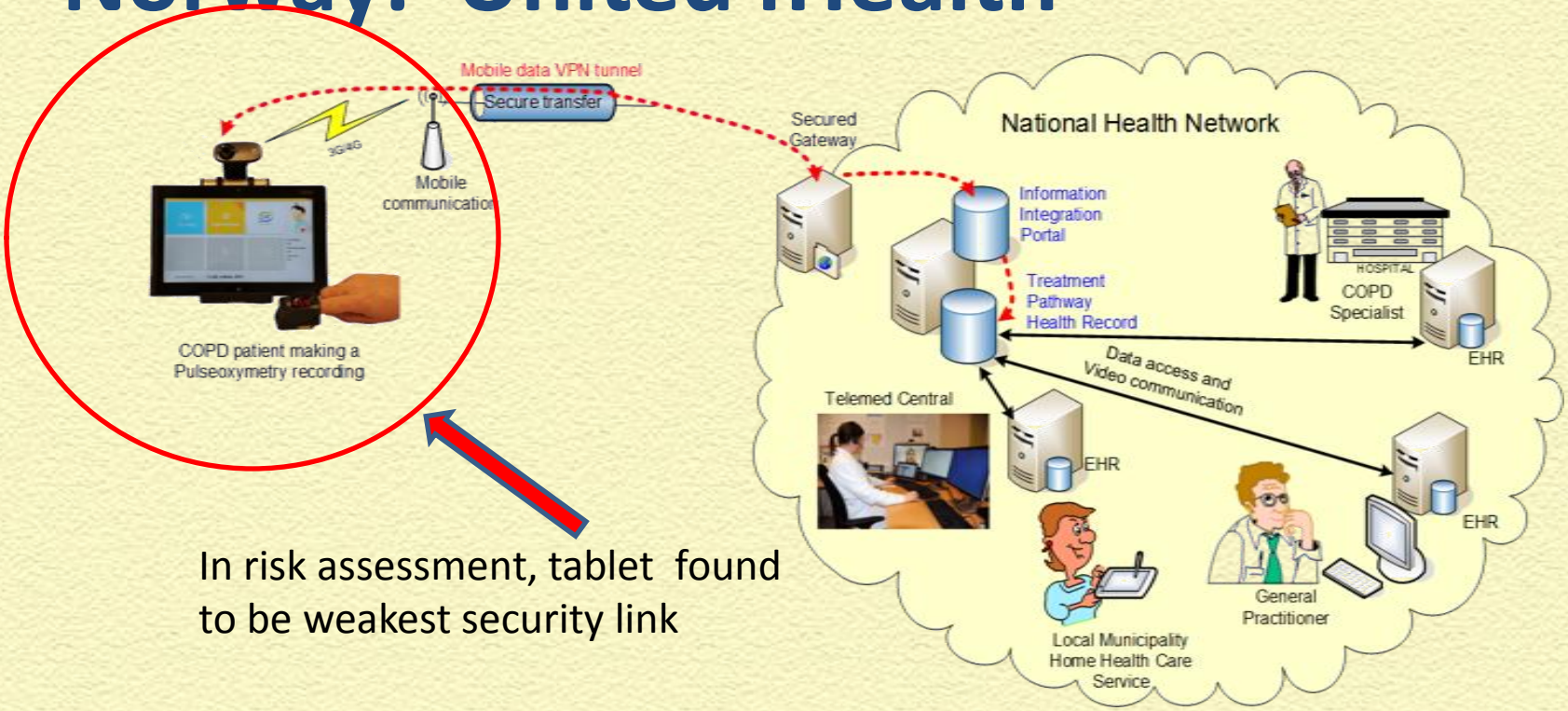
# mHIMSS Best Practice Recommendation

- Encrypt data at rest and in transit (AES 128/256; no more than 64 if for export)
- Do a risk assessment to determine weak points and design security policy accordingly

- More information at mHealth Roadmap

http://www.himss.org/ResourceLibrary/mHimssRoadmap

# Norway: United4Health




In risk assessment, tablet found to be weakest security link

Solution: uses VPN SSL, web based secure connection (https); tablet functionality is locked down to only telehealth application use; user access security software on tablet; all data is encrypted at rest on tablet and in transmission to Health Network; de-identified data is transmitted from the tablet; two factor authentication methods are used; not using all of Continua guidelines

# Summary

- Need to at least ensure confidentiality, integrity and authentication of 5 A's
- Continua offers guidelines for implementation of security standards at interfaces
- mHIMSS recommendation is to encrypt at rest and transit; do a risk assessment to determine policy
- Is evolving as technology evolves

- Questions?

- Thank you

Bridget A. Moorman, CCE, Consultant
Mhealth Competence Centre of Mobile World Capital Barcelona
bridget@bmoorman.com