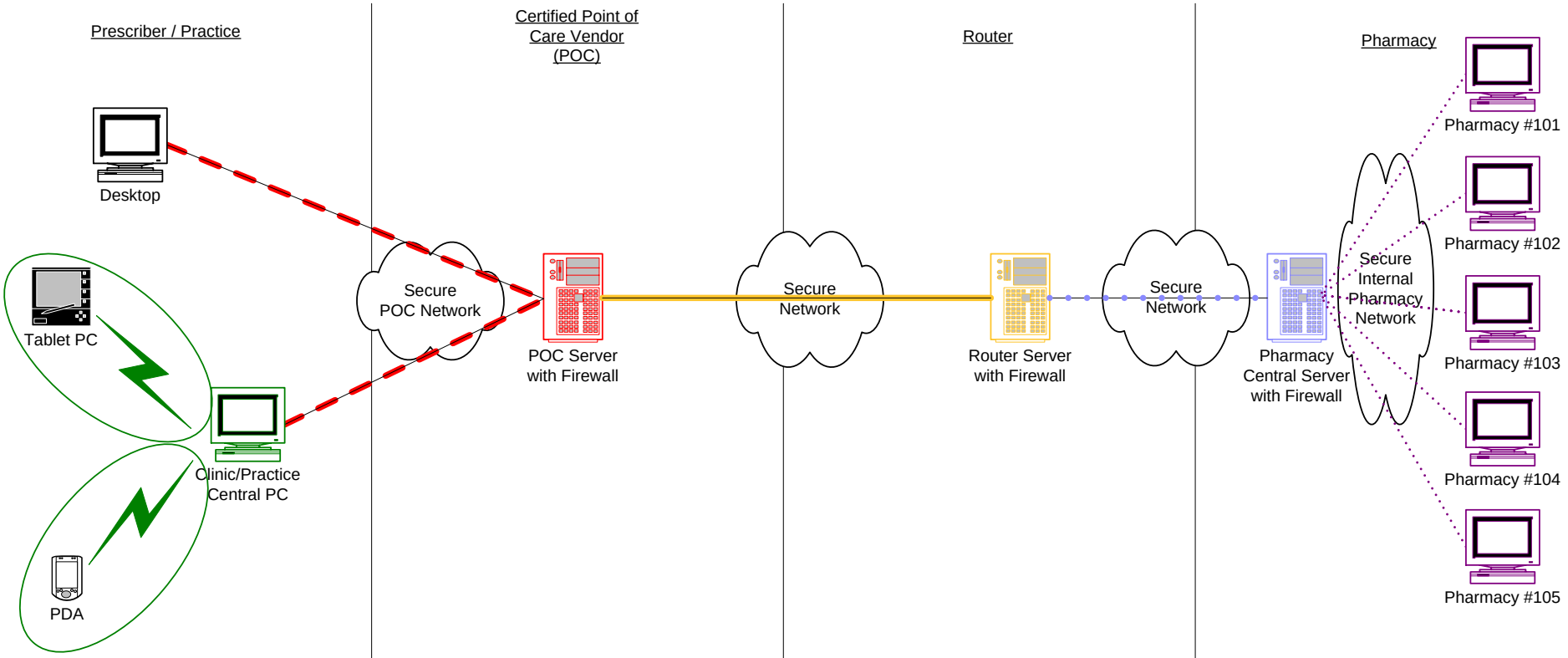
Electronic Prescribing Security and Authentication

December 9, 2004

Phillip A. Rothermich
VP, Business Development
Express Scripts, Inc.
13900 Riverport Drive
Maryland Heights, MO 63043
(314) 702-7109
(314) 702-7657 fax
prothermich@express-scripts.com

Terri A. Swanson
CIO
CIGNA Pharmacy Management
900 Cottage Grove Road, S323
Hartford, CT 06152
(860) 226-2988
(860) 226-5713 fax
terri.swanson@cigna.com

Electronic Prescribing Security and Authentication Standards



-- Authentication: POC authenticates prescribers before assigning unique IDs to them (IDs are unknown to prescribers).
-- Security: Authenticated prescribers are granted access to POC technology, where they login with unique usernames and passwords.
-- Security: Prescribers send prescription data to POC server through POC's secure channel ( ).
-- Under one or more contractual relationships, POC and Router are authorized to transmit the eRx on behalf of the physician to the pharmacy.
-- Wireless technologies (e.g. tablet PCs and PDAs) contain their own security profiles to prevent unauthorized access or interception ( ).

-- Authentication: POC and Router verify each other's static IP addresses, IDs and passwords before opening secure channel for transporting an eRx.
-- Security: Prescriber initiates eRx being sent from the POC server to the Router server through the Router's https secure channel ( ).
-- Security: POC performs internal assessments using security scanning tools for network and system security.
-- Security: Use of PHI (protected health information) must be in accordance with HIPAA standards for the purpose of treatment, payment or healthcare operations.

-- Authentication: Router verifies the IP addresses, IDs and passwords of each participant (POC and Pharmacy) before opening secure communication channels.
-- Security: Router adheres to security policies which are consistent with HIPAA security guidelines.
-- Security: Router performs internal assessments using security scanning tools for network and system security.
-- Security: Router maintains only enough information to allow for routing, auditing and support.
-- Security: Router may not view or modify eRxs, except when translating from one messenging standard to another (e.g. HL7 to NCPDP).

-- Authentication: Pharmacy and Router verify each other's IP addresses, IDs, and passwords before opening a secure channel ( ) for transporting eRxs.
-- Authentication: Pharmacy stores a cross-reference table containing DEAs and their unique IDs (assigned by POC or Router).
-- Audit Trail: Pharmacists may contact a POC or prescriber at any time to verify the authenticity of an eRx.
-- Audit Trail: POC, Router and Pharmacy maintain transaction logs that may be used for auditing purposes.
-- Authentication: Pharmacy (Central Server) and each Pharmacy site verify each other's IP addresses, IDs, and passwords before opening a secure channel (.....) for transporting eRxs.

What is Security/Authentication?

What is "Security"?

- **Systems or procedures that ensure that prescription information cannot reasonably be accessed, modified or redirected by an unauthorized person.**

What is "Authentication"?

- **Providing an auditable process upon which a dispensing pharmacist can rely to ascertain, to a reasonable degree of certainty, that the person identified as the author of a prescription received (i) is in fact the prescriber of that prescription and (ii) could not reasonably repudiate his or her authorship.**

Overview: Electronic Prescribing Today

- **Provides HIPAA-level security if not better.**
- **Provides significantly more reliable methods of authentication than existing processes.**
- **Is hampered by patchwork of incomplete or unclear state rules and regulations that haven't kept up with evolution of technology.**
- **Is threatened by proposals to require security and authentication processes which are impractical to implement and are beyond those applicable to other healthcare records.**

Security: What does HIPAA "require" of a Covered Entity to achieve "Security" of Protected Health Information

Requirement	Description	eRx
Administrative Safeguards	• prevent, detect, document, contain and correct security violations; • determine appropriate, limited access to be given to identified individuals; • ensure workforce training regarding security policies; • provide planned response to threatening occurrences (natural disasters, vandalism, etc.); • implement periodic technical testing and evaluations.	✓
Physical Safeguards	Appropriately limit physical access to electronic information systems, hardware, software and facilities in which they are housed against unauthorized access.	✓
Technical Safeguards	Implement unique names/numbers to track access; emergency access procedures; audit controls that record and examine system access and activity; protection against improper alteration/destruction; procedures to authenticate user access; measures to protect information being transmitted against unauthorized access or modification without detection. Note: Current industry standard is SSL ("channel encryption"); encryption of data during transmission is "addressable", not "required".	✓
Organizational Safeguards	Enter into Business Associate contracts with all applicable entities obligating them to comply with similar requirements.	✓
Documentation Requirements	Document policies and procedures applicable to the foregoing, including actions taken and assessments made; such documents must be retained for six (6) years, appropriately made available, and reviewed periodically for updates/revisions.	✓

Security Comparison

Paper Rx

- Minimal

Rx by Fax

- Minimal

Rx by Phone

- Minimal

eRx

- Prescribers are required to **login** to POC system with unique usernames and passwords
- eRx travels through encrypted (128-bit minimum) and **secure channels**
- POCs, routers and pharmacies perform regular **internal security assessments** of their servers
- Compliant with **HIPAA** security guidelines
- Risk of alteration is minimized and audit trail provides ability to find source of any alteration

BOTTOM LINE:

The security available through electronic prescribing is significantly better than that available today, and is sufficient to protect the privacy of the individuals involved.

Why is authentication of an electronic prescription a concern for pharmacists?

- State Boards of Pharmacy hold pharmacists responsible for determining the authenticity of a prescription before it is filled.
- Failure to follow applicable regulations defining what is or is not a valid prescription could jeopardize a pharmacist's license.
- Many state regulations are based on established methods for writing prescriptions on paper and/or transmitting prescriptions via facsimile or telephone.
- Where guidance exists with respect to e-Rxs, state regulations often require the e-Rx to contain some form of mark or "electronic signature" (loosely defined) that "authenticates" the prescription – this does not provide the pharmacist with clear guidance, nor do such marks necessarily provide substantive authentication.

BOTTOM LINE:

Pharmacists are often reticent to accept electronic prescriptions without telephonic verification unless state board of pharmacy approves specific application or process. Focus needs to be on substantive authentication rather than "electronic signature".

Authentication Comparison

Paper Rx

- Wet **signature**

Rx by Fax

- Image of **signature**
- Caller ID / **fax** number

Rx by Phone

- Caller ID / **phone** number

eRx

- POCs verify prescribers' **DEA numbers and state licenses** before allowing them to write eRxs
- POC, router and pharmacy servers verify each other's static **IP addresses, IDs and passwords** before opening secure channels for each eRx
- **Prescriber Unique ID** for ePrescribing
- Prescriber **phone** number
- Prescriber **fax** number
- Transaction logs are kept and provide auditable record

BOTTOM LINE:

Current electronic prescribing processes provide reliable methods for authenticating the validity of prescriptions created and sent via such a system.

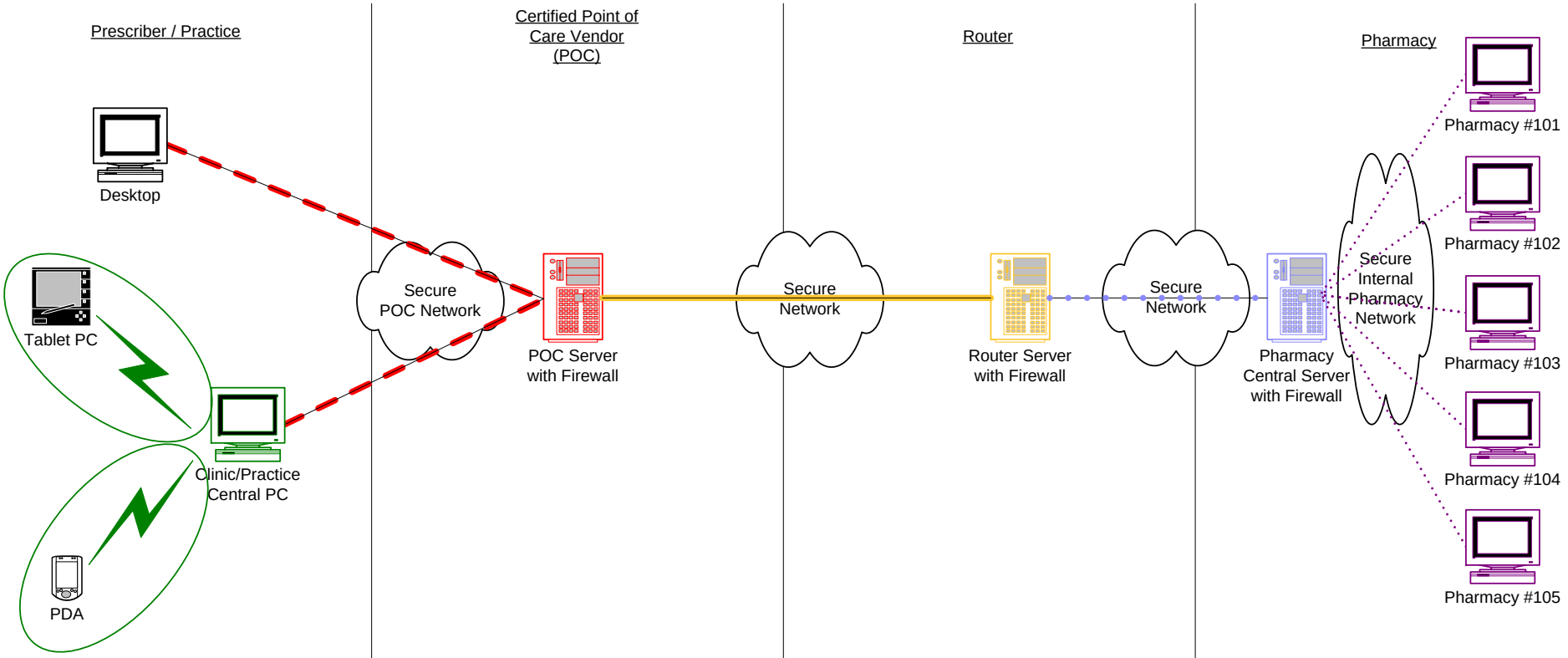
PKI Digital Signature Is Impractical to Implement for eRx

- Doesn't provide significant additional security or authentication
- Potential barrier to **translation** of data for interoperability (i.e., HL7 to NCPDP)
- **Cost-prohibitive**
- **Administrative burden** – every prescriber must share "key" with every pharmacy – one-to-one solution

Solution:

1. Adopt existing best practices as standards requiring all participants in electronic prescribing environment to implement them as minimum level of security and authentication measures.
2. Clarify by rule that these standards supersede state laws and regulations relating to security or authentication of electronic prescriptions, based on authority in MMA for preemption of any law or regulation which is contrary to the standards or restricts the ability to carry out the electronic prescribing program.
3. Implement certification process to annually validate compliance with the standards such that scripts sent via a certified system are deemed valid for purposes of provider authentication and fulfillment.

Electronic Prescribing Security and Authentication Standards



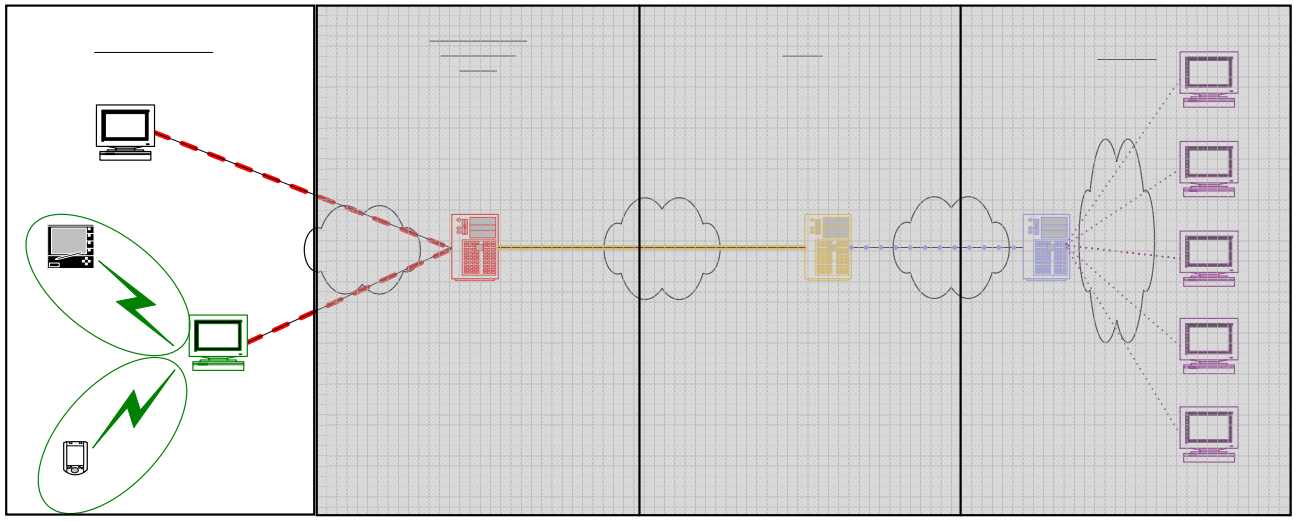
-- Authentication: POC authenticates prescribers before assigning unique IDs to them (IDs are unknown to prescribers).
-- Security: Authenticated prescribers are granted access to POC technology, where they login with unique usernames and passwords.
-- Security: Prescribers send prescription data to POC server through POC's secure channel ( ).
-- Under one or more contractual relationships, POC and Router are authorized to transmit the eRx on behalf of the physician to the pharmacy.
-- Wireless technologies (e.g. tablet PCs and PDAs) contain their own security profiles to prevent unauthorized access or interception ( ).

-- Authentication: POC and Router verify each other's static IP addresses, IDs and passwords before opening secure channel for transporting an eRx.
-- Security: Prescriber initiates eRx being sent from the POC server to the Router server through the Router's https secure channel ( ).
-- Security: POC performs internal assessments using security scanning tools for network and system security.
-- Security: Use of PHI (protected health information) must be in accordance with HIPAA standards for the purpose of treatment, payment or healthcare operations.

-- Authentication: Router verifies the IP addresses, IDs and passwords of each participant (POC and Pharmacy) before opening secure communication channels.
-- Security: Router adheres to security policies which are consistent with HIPAA security guidelines.
-- Security: Router performs internal assessments using security scanning tools for network and system security.
-- Security: Router maintains only enough information to allow for routing, auditing and support.
-- Security: Router may not view or modify eRxs, except when translating from one messenging standard to another (e.g. HL7 to NCPDP).

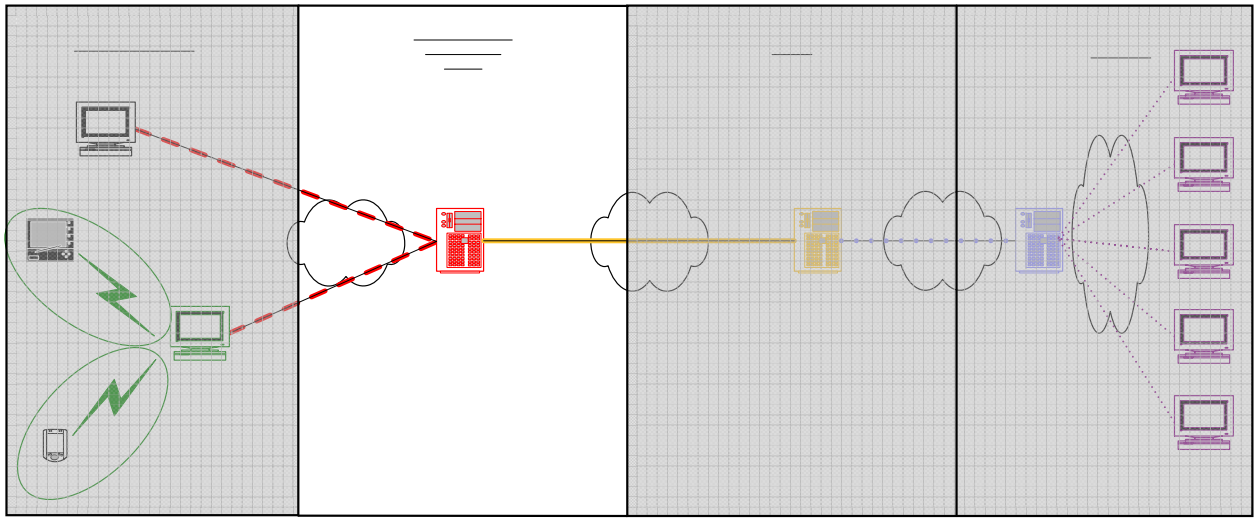
-- Authentication: Pharmacy and Router verify each other's IP addresses, IDs, and passwords before opening a secure channel ( ) for transporting eRxs.
-- Authentication: Pharmacy stores a cross-reference table containing DEAs and their unique IDs (assigned by POC or Router).
-- Audit Trail: Pharmacists may contact a POC or prescriber at any time to verify the authenticity of an eRx.
-- Audit Trail: POC, Router and Pharmacy maintain transaction logs that may be used for auditing purposes.
-- Authentication: Pharmacy (Central Server) and each Pharmacy site verify each other's IP addresses, IDs, and passwords before opening a secure channel (.....) for transporting eRxs.

Electronic Prescribing Security and Authentication Standards



Prescriber / Practice

Electronic Prescribing Security and Authentication Standards



Prescriber / Practice

Certified Point of Care Vendor (POC)

Router

Desktop

Secure POC Network

Secure Network

Secure Network

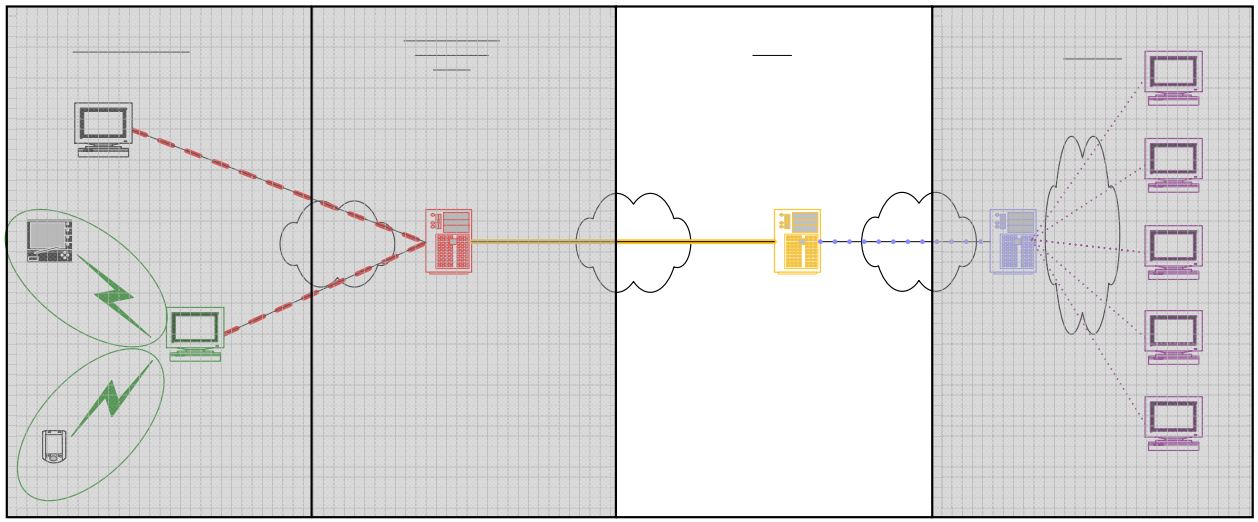
Tablet PC

POC Server with Firewall

Router Server with Firewall

Electronic Prescribing Security and Authentication Standards

Router



Prescriber / Practice

Certified Point of Care Vendor (POC)

Router

Desktop

Tablet PC

Secure POC Network

POC Server with Firewall

Secure Network

Router Server with Firewall

Secure Network

Pha
Centra

Electronic Prescribing Security and Authentication Standards