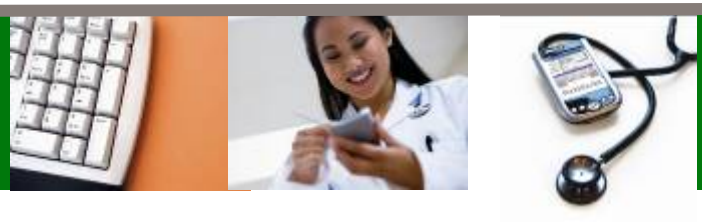
zixcorp



EPCS Presentation

Nigel Johnson
VP Product Management and
Business Development

Maximize safety
Optimize workflow
Minimize costs

Zix Corporation – Company Overview

NASDAQ-listed company with 210+ employees, based in Dallas, Texas

Secure Email

- Leader in healthcare
- 5 million protected email accounts
- 800 enterprise-wide email encryption customers
- Enables HIPAA-compliant transmission of PHI

e-Prescribing

- End-to-end certified connectivity with RxHub and SureScripts
- High touch deployment model that results in strong physician adoption and utilization

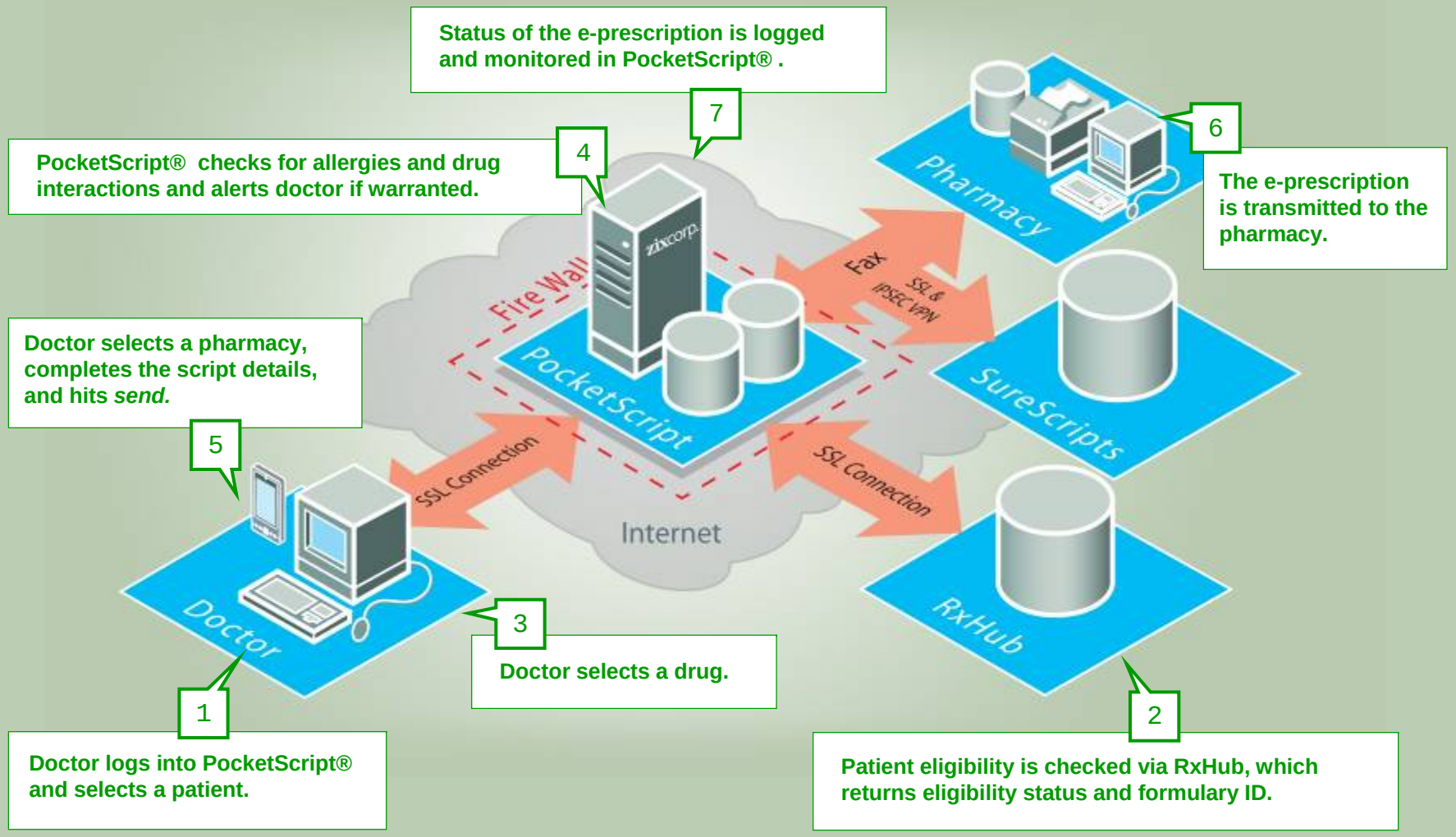
ZixData Center™

Secure Technology Platform: 99.99% availability

- Trusted third party (SysTrust and SAS-70 certified)
- 7x24 data center and services monitoring
- 1.3 million prescriptions in Q206
- 100,000 prescriptions per week

zixcorp.

PocketScript Connectivity



Risks

- There are two security risks in e-prescribing:
  - Unauthorized prescribing
  - Unauthorized access to sensitive information
- These are addressed by:
  - Following the “Second set of Recommendations on ePrescribing Standards” from the NCVHS
  - SAS–70 Type II certification
  - AICPA SysTrust certification
  - Annual audits by the “Big 4” on:
    - Security
    - Availability
    - Processing Integrity
    - Confidentiality

Controlled substance risks

- SysTrust and SAS-70 certification mean the risk is not increased for controlled substance electronic prescribing
- E-prescribing is superior to the current system:
  - Prescribing pads can be stolen
  - Written prescription information can be modified
  - Written prescriptions can be forged
- Electronic prescriptions allow for:
  - Fast easy audits
  - Immediate shut down of problem prescribers
- Therefore, there is no need to make changes for controlled substance electronic prescribing

Authentication

- The most important step of any security system
- ZixCorp does the following for authentication
  - We validate the identity of the doctor by visiting their practice
  - Every user has a unique ID and password
  - Different levels of users with different capabilities
    - Doctors, nurses and MAs
  - Passwords are forced to be complex
  - Three strikes policy
  - Audit logs are kept for all password resets
- In addition, all of our partner connections are authenticated

Prescription Integrity

- Prescription records are protected by:
  - Policy
  - Software (logging and auditing)
  - Geographic separation
- The data center is:
  - Manned 24/7
  - In the 4th security level of a 4 zone system
  - Accessed only through badge access and biometric scanning
  - All staff undergo comprehensive background checks

Current and Future Threats

- The system is specifically designed to eliminate the threats of:
  - Eavesdropping
  - Man in the middle attacks
  - Hijacking, and
  - Impersonation
- The required security design elements are all demanded by SysTrust and SAS-70 and are also handled by our authentication policies and the policies of RxHub and SureScripts.

Smart Cards and PKI Comments

- Smart cards and PKI can implemented, but…
- They are very expensive to implement across all the vendors in the chain:
  - Point of care vendors
  - Pharmacy connection networks
  - Pharmacy systems
- In addition the PKI elements must work on all platforms and versions. This include, browsers, handhelds, mainframes and UNIX servers
- Cross-certification of CAs has historically not worked well in private industry.

Conclusion

- Allowing electronic prescription of Schedule II drugs will speed adoption of e-prescribing
- Forcing the adoption of PKI will slow the adoption of e-prescribing