

Remote Servicing under HIPAA with proposed Solution A

John F. Moehrke

Chairmen of Remote Servicing Focus Group
NEMA/COCIR/JIRA Security and Privacy
Committee

Systems Engineering – Security and Privacy in
Healthcare

GE Medical Systems

HIMSS – January 28, 2002

What you will learn today

- Remote Servicing is critical
- Remote Servicing presents new security risks
- Vendors are working on a common solution that will
 - a. Reduce administration (Hospital and Vendor)
 - b. Improve Accountability
 - c. Provide a more secure environment

Security and Privacy Committee (SPC)

- Joint effort by NEMA-MII, COCIR-IT, and JIRA
- Mission: Ensure a level of data security and data privacy in the health care sector that:
 - Meets legally mandated requirements
 - Can be implemented in ways that are reasonable and appropriate
 - Reduces Healthcare costs of compliance
- Scope: All systems, devices, components, and accessories used in medical imaging informatics
- Scope is not exclusive of other products and is expected to be extendable to all Equipment that maintains Patient Data (PHI)
- International data security and data privacy legislation, currently focusing on the European Community, Japan, and the United States of America

Efforts of the SPC

- Educational Document :
 - <http://medical.nema.org/privacy/education.pdf>
- Remote Servicing Proposal (This talk)
 - <http://medical.nema.org/privacy/remote.pdf>
- Audit Controls:
 - <http://medical.nema.org/privacy>
- Secure IHE Profiles
 - Work in progress
- Members: AGFA, GE, Kodak, Konica,
Dhilon, Siemens, Toshiba

Why do Remote Servicing?

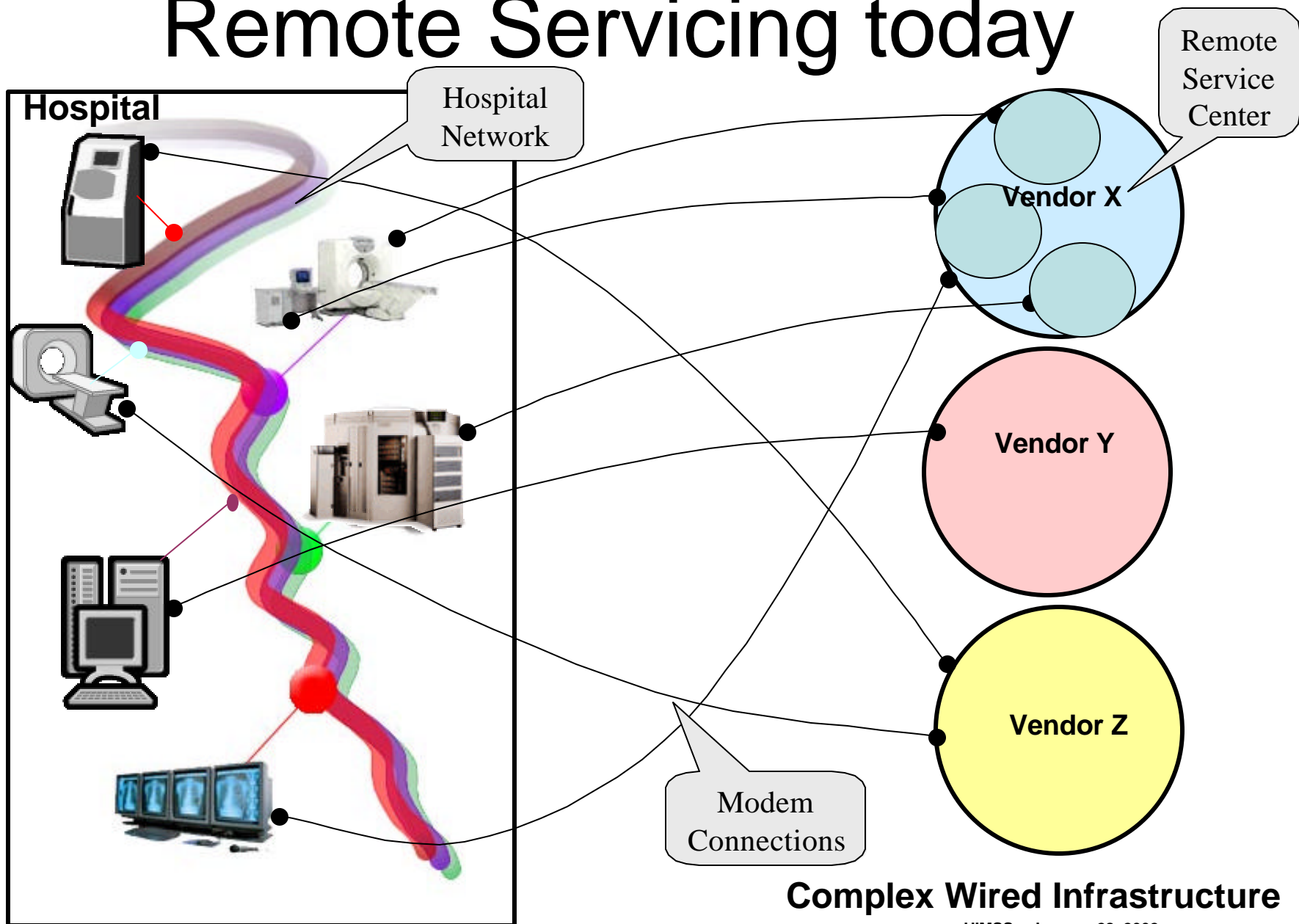
Benefit to Health Care Provider

- Better Availability and Integrity of the systems
- Quick response as no Travel involved
- Higher quality of service
 - Knowledge base available at the Vendor
 - Expert can be applied to the problem/solution

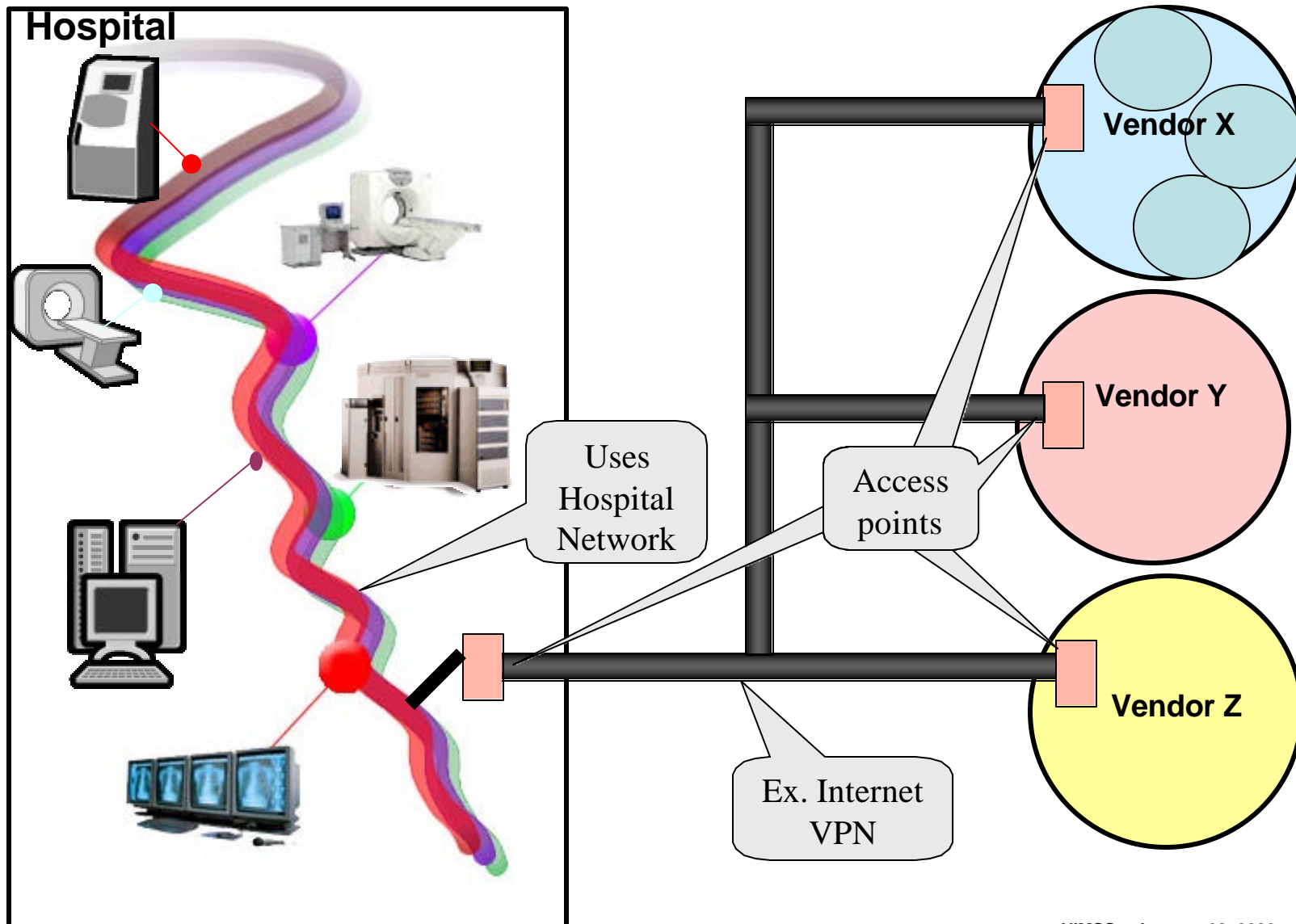
Benefit to Vendor

- Lower costs to service equipment

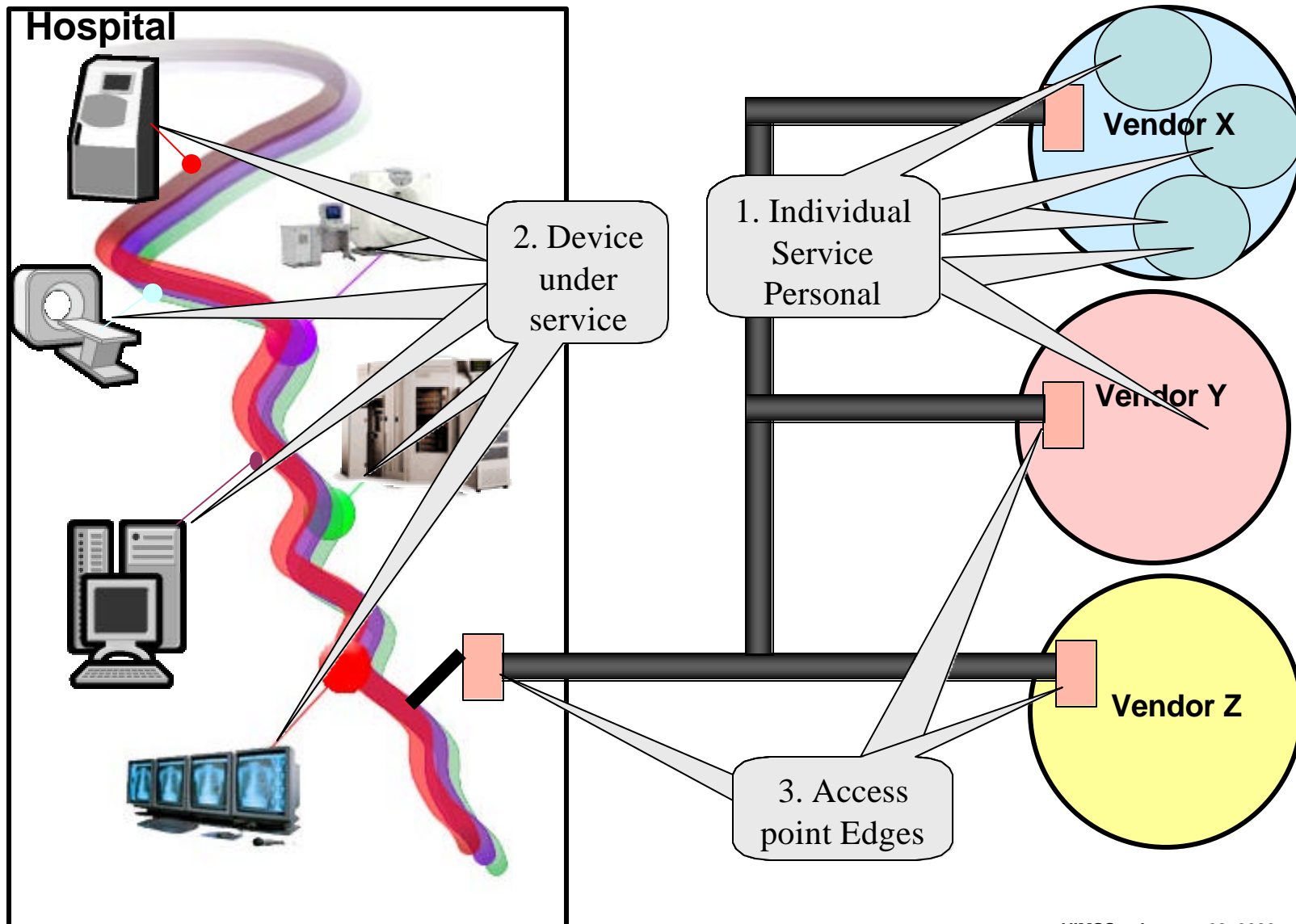
Remote Servicing today



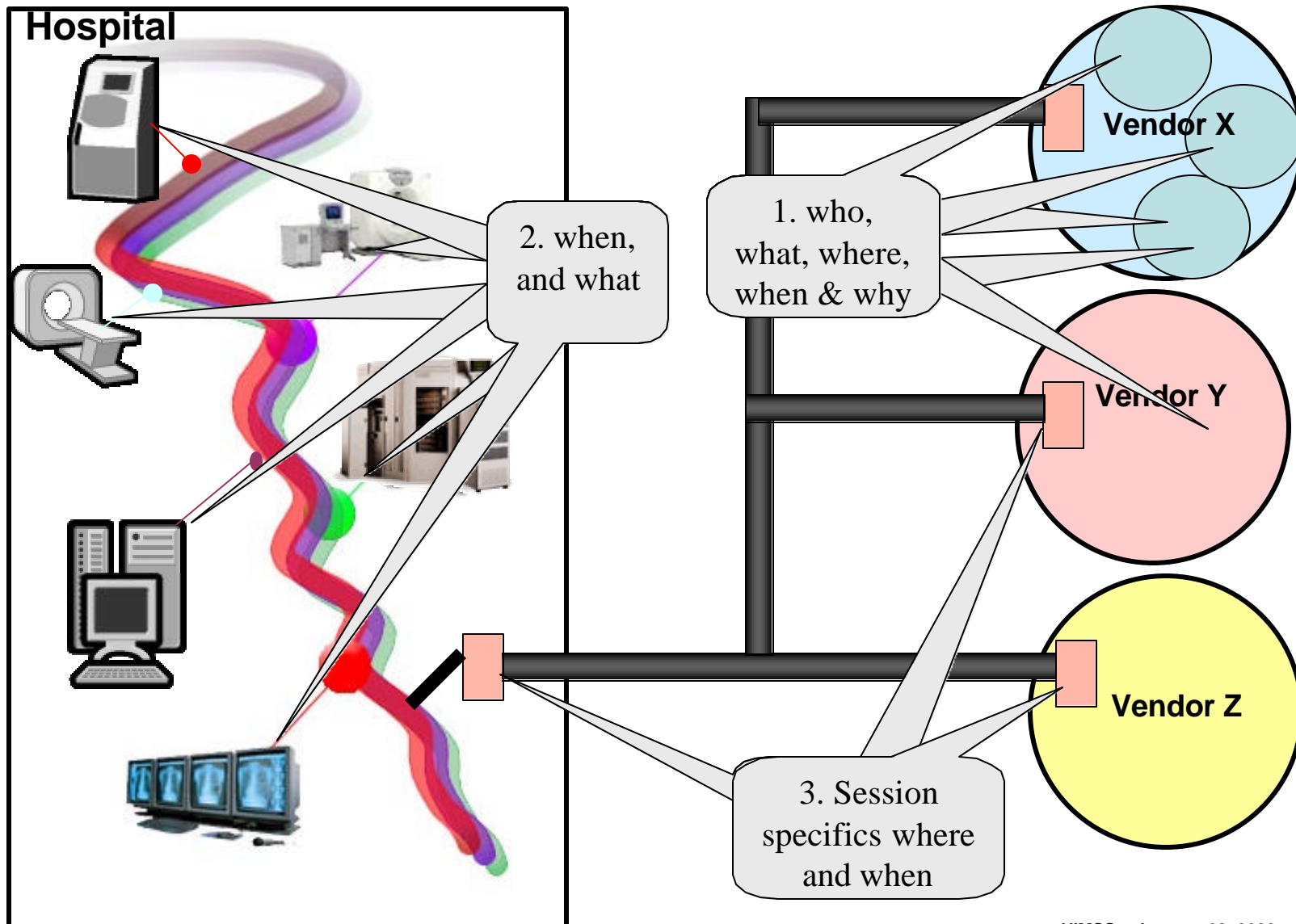
Remote Servicing Solution



Access Control



Audit Trails



Health Care Provider gains Control and Manageability

- Control of each session and/or vendor
- Rules that restrict where vendor X can go, what tools they can use, when they can connect, etc
- Strong Access Point Authentication
- Audit trails to prove accountability

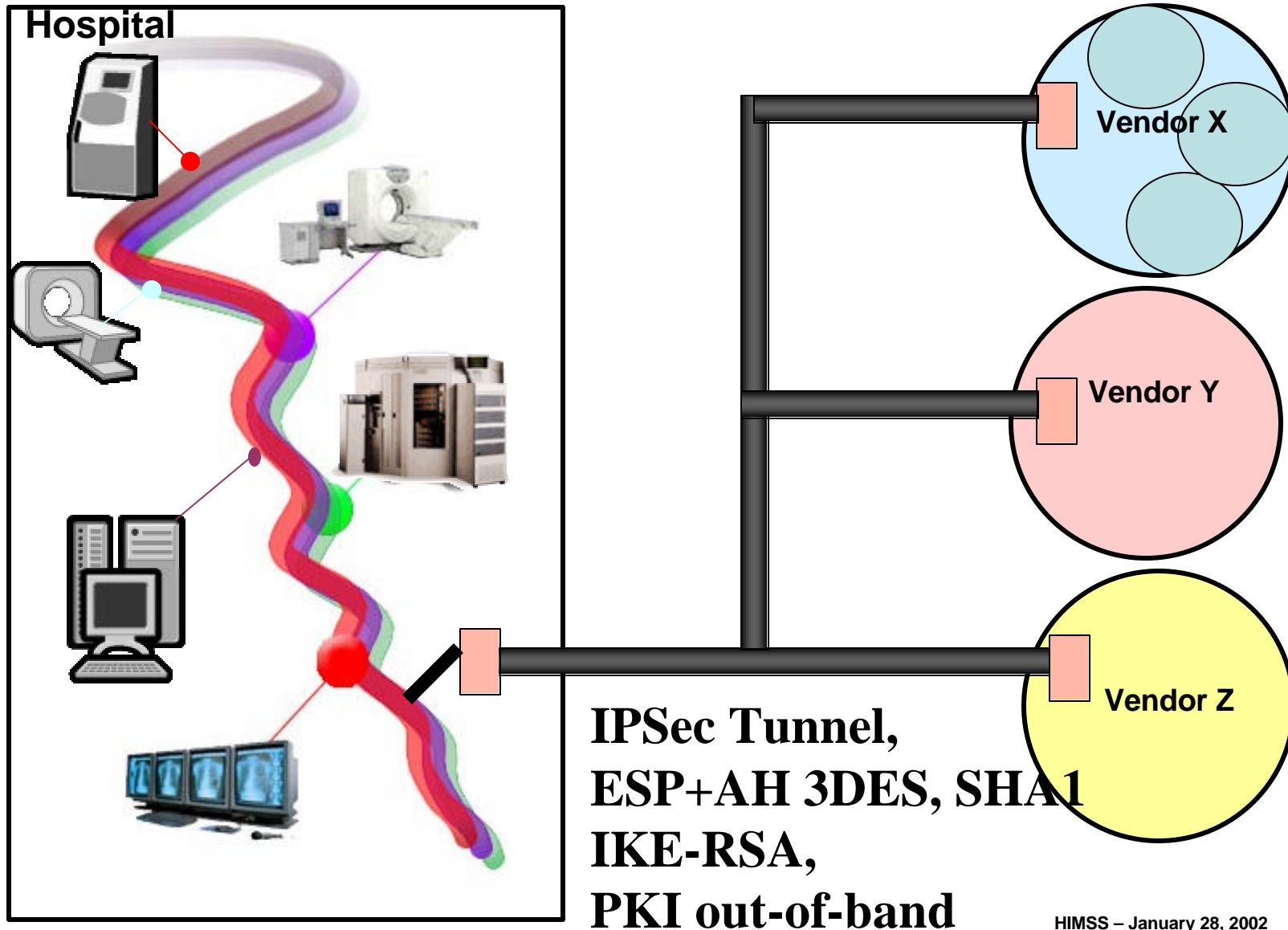
Next Steps for SPC

→ Focus Group Charter

Define a Reasonable and Practical solution that follows this architecture

- Candidate 'A' -- IPSec tunneling over the Internet
 - ESP/AH – 3DES and SHA1
 - IKE – Session Key negotiation
 - Certificates – communicated out-of-band (mail, courier, etc)
 - Filtering and Routing rules maintained by the Healthcare facility
 - Audit trails maintained at RSC
 - Individual Authentication maintained at the RSC

Solution A: IPSec on Internet



Conclusion

- The Focus Group is actively creating these Descriptions of Candidate Implementations
 - Vendors are providing experts from their Service organizations
 - AGFA, GE, Kodak, Philips, Siemens, Toshiba, +
- Targeting End of 2002 with demonstration at RSNA
- Will seek approval by NEMA, COCIR, and JIRA early 2002

John F. Moehrke

GE Medical Systems

262-293-1667

John.Moehrke@med.ge.com