

Comments on 21 CFR Part 11

Public Meeting on Electronic Record; Electronic Signatures (Part 11)

NTSB Conference Center, Washington, DC

June 11, 2004



Haruhiko Araki

Consultant,

Pharma & Biotech Systems Dept.,

Total Solutions Div.,

 **Hitachi, Ltd.**

Introducing Hitachi and Its Subsidiaries

- ◆ **Supplying various computer/computerized systems to pharmaceutical/food industries**
- ◆ **Offering consultation services to those industries**
- ◆ **Exporting medical devices worldwide**
 - Automated Biochemical Analyzers (OEM)
 - Advanced clinical diagnostic systems
e.g. MRI^{*1}, PET^{*2}, Optical Topography,
and MCG^{*3} (near future)
 - Proton Beam Therapy System (under construction in TX)

*1: Magnetic Resonance Imaging

*2: Positron Emission Tomography

*3: Magneto-Cardiogram

- ◆ **Comments on the scope of Part 11**
- ◆ **Comments on the audit trail provision**
- ◆ **Comments on open/closed system differentiation**

Topics IV.A.1., IV.A.3., IV.D.2.

- ◆ *Should Part 11 be revised to implement the narrow interpretation?*
 - Yes, please!! Because a ‘Guidance’ does not “establish legally enforceable responsibilities”
- ◆ *Need to clarify records not specifically identified but still required in predicate rules?*
 - Not necessarily in Part 11, however, more explicit clarifications are expected.
... maybe in additional guidance(s) because ...

Room for Interpretation Still Resides in GLP

◆ 21 CFR Part 11 Sec. 11.1 (b)

- *“This part also applies to electronic records submitted to the agency ... even if such records are not specifically identified in agency regulations.”*

◆ 21 CFR Part 58 (GLP) Sec. 58.3 (d)

- *“Nonclinical laboratory study means in vivo or in vitro experiments ... under laboratory conditions to determine their safety.”*

[conventional interpretation of the scope]

- TOX
- concomitant TK
- Core Battery (of safety pharmacology)

◆ ICH M4S (The CTD -- Safety)

- Primary/secondary pharmacodynamics and PK are also included.



Shall raw data in PDs and PK be Part 11 compliant?

... or, only final reports and datasets attached to applications?

- ◆ **Comments on the scope of Part 11**
- ◆ **Comments on the audit trail provision**
- ◆ **Comments on open/closed system differentiation**

Topic IV.D.4.

◆ ***Potential changes that would encourage innovation?***

- ‘*Scope and Application*’ Sec. III.C.2.
 - *“Persons must still comply with all applicable predicate rule requirements ... as well as any requirements for ensuring that changes to records do not obscure previous entries.”*
- 21 CFR Part 58 (GLP) Sec. 58.130 (e)
 - *“Any change ... shall be made so as not to obscure the original entry, ...”*
- ICH E6 (GCP) Sec. 4.9.3
 - *“Any change or correction to a CRF ... should not obscure the original entry”*
- ICH Q7a (GMP for APIs) Sec. 6.14
 - *“... Corrections to entries should ... leave the original entry still readable.”*



**“Changes shall not obscure the previous entry”
seems to be GxP requirement.
Need to duplicate it in Part 11?**

Innovative Diagnostic Equipments

◆ Electronic Imaging Technology changes PD/PK

- Imaging Plate (invented by Fujifilm) w/ imaging analyzer
→ 10^3 broader dynamic range than X-ray films
- MRI, PET, SPECT (Single Photon Emission CT)
→ Already used in medical scenes (implies high risk to patients)
i.e. validated, security features furnished
- An image is merely a type of representation of 3-D numerical data.
→ Some info. would be lost in printed copies

◆ In general, computer system security permits “overwriting” data when authorized.

- User authentication and access control are the ‘musts’, audit trails are desired. *Note: audit trails are meaningless without auditing them!*
- All you need is recent OS ... Win2k or later can realize it.
- rf. TCSEC(DoD 5200.28-STD, 1985), ISO/IEC 17799:2000

Assuming PD/PK are still non-GLP...

...and Part 11 is implicitly required for raw data in PD/PK;

- ◆ **Saving all history data may require terabytes!**
 - It implies additional costs \$100,000s ... might restrain innovation.
- ◆ **Risks to human patients are yet uncertain when PD/PK studies are conducted.**
- ◆ **An appropriate Security Management System has ‘safeguards’.**
 - Effective in medical scenes.
 - Suspected data can be identified and excluded.
- ◆ **No objection to reserving predicate rule requirements.**



Do we still need this, in Part 11?

“... Record changes shall not obscure previously recorded information.”

- ◆ **Comments on the scope of Part 11**
- ◆ **Comments on the audit trail provision**
- ◆ **Comments on open/closed system differentiation**

Topics IV.B.4., IV.D.8.

◆ “*open system*” ... confusing

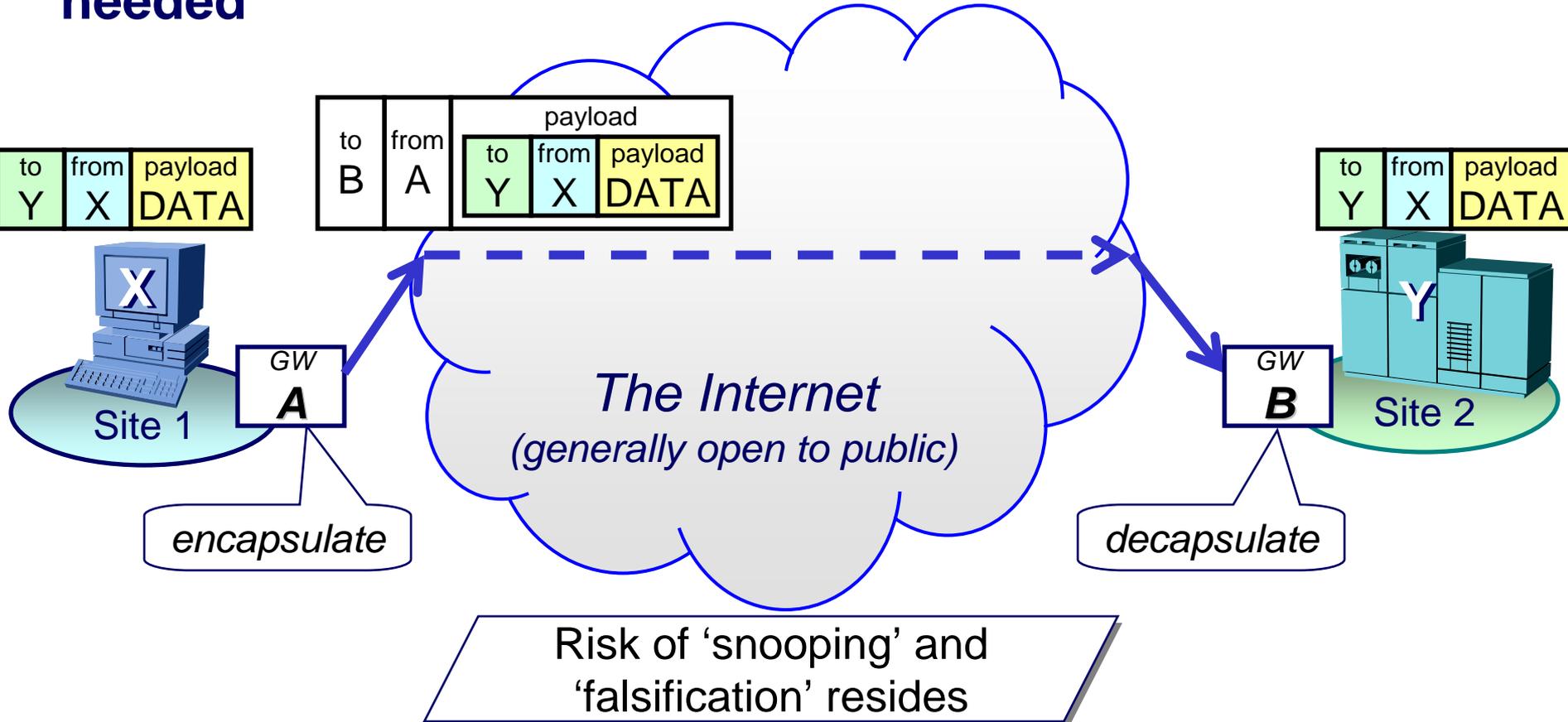
- Computer: *a system of which interface spec. is available to public*
- Science: *a system that (energy) flows are not ended inside*
- Building: *a type of contraction that more than one builder are equally ordered (by a customer)*
- Part 11: *only Sec. 11.30 refers to it*

◆ Technologies and Concepts after Part 11 Effective Date

- IPsec (Security Architecture for the Internet Protocol)
 - RFC2401 (1998, updated by RFC3168)
- VPNs based on MPLS (Multiprotocol Label Switching)
 - RFC2547 (1999), RFC2917 (2000), RFC3031 (2001), etc.
- VPN White Paper
 - “VPN Technologies: Definitions and Requirements”, VPN Consortium, 2003
- ISMS (Information Security Management System) standards
 - BS7799:1999, BS7799-2:2002
 - ISO/IEC 17799:2000

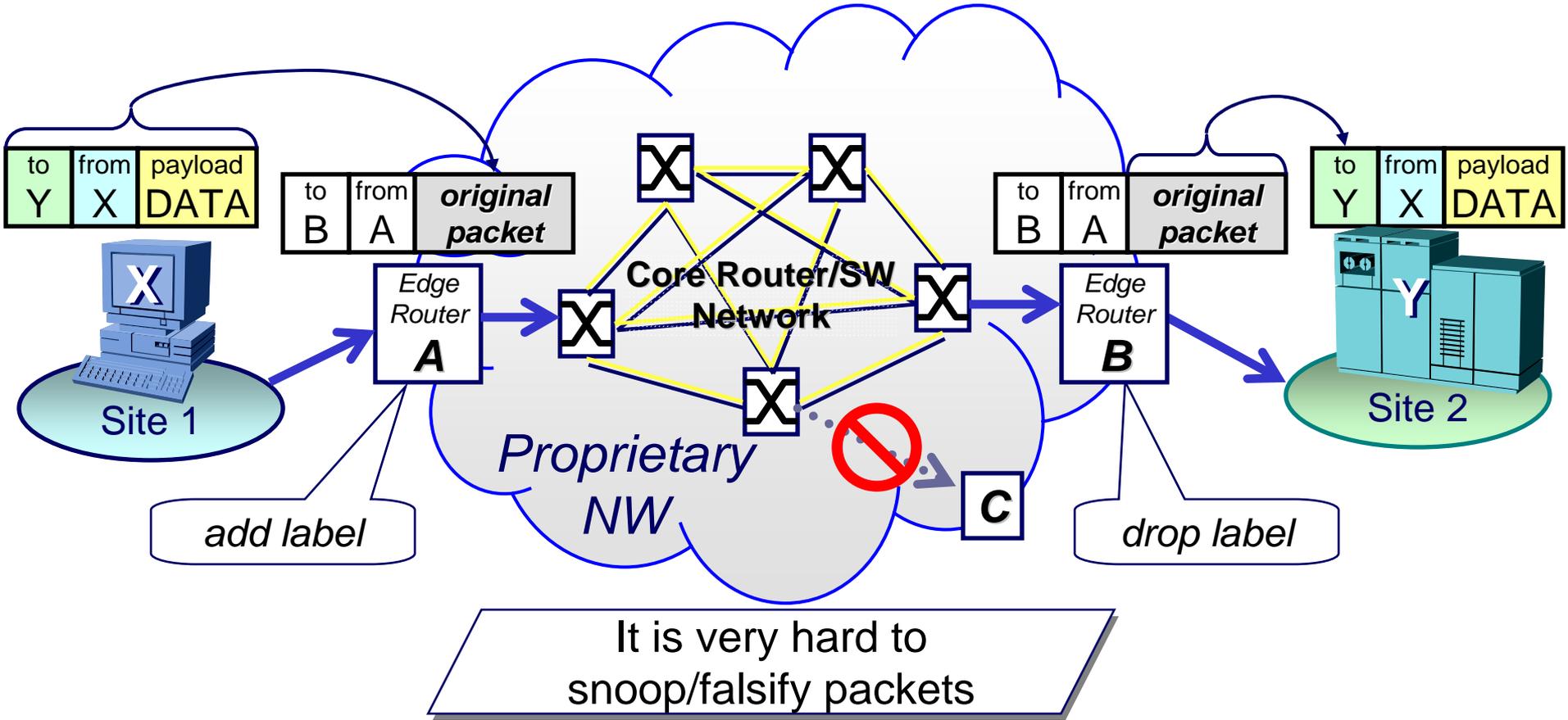
Primitive VPN

- ◆ “open system” because nobody entirely controls Internet
- ◆ Additional measures e.g. encryption / digital signature needed



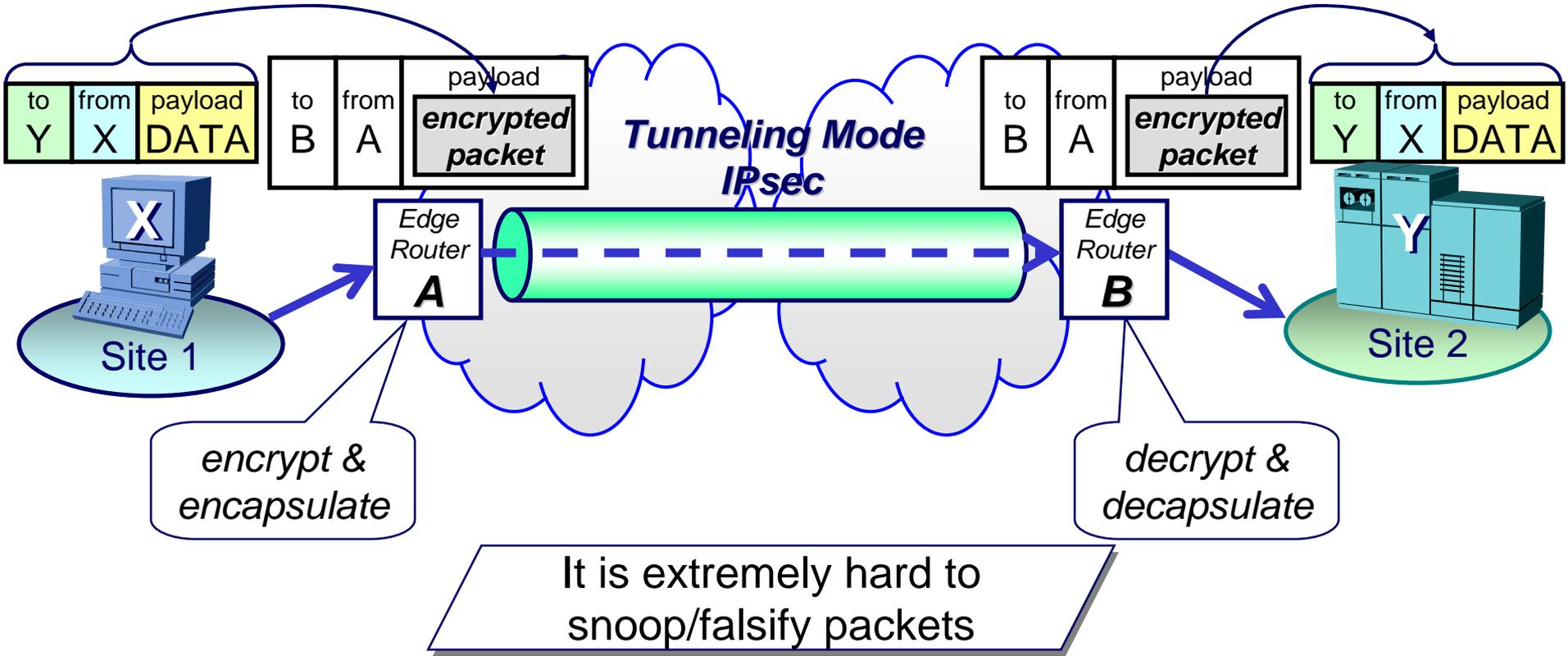
“Trusted VPN” by MPLS

- ◆ “open system” because NW is operated by a provider
- ◆ Data security & integrity are ensured by the provider



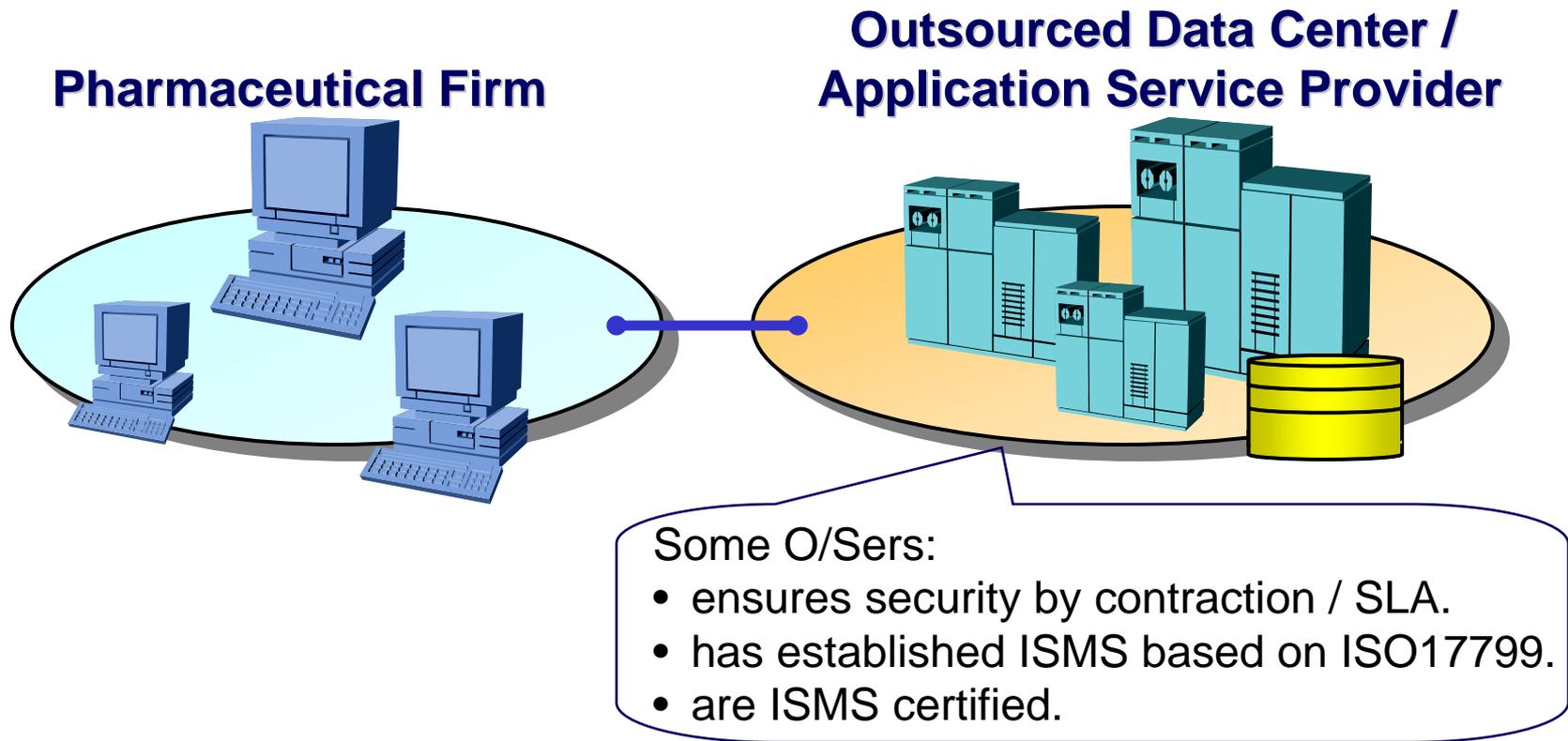
“Secure VPN” by IPsec

- ◆ “open system” because NW is operated by a provider
- ◆ Data security & integrity are strongly ensured by the provider



Outsourcing System Access Control

- ◆ “open system” by definition in Sec. 11.3 (9)
- ◆ Outsourcers are often required to ensure security by their sponsor.



Suggestion

- ◆ **No more ‘open’/‘closed’ system definitions**
- ◆ **Title of Sec. 11.10 → “Controls for ER systems”**
- ◆ **Sec. 11.30 → Sec. 11.10 (I)**
 - “When access to an entire or a part of system is controlled by persons who are not responsible for the content of electronic records, one or more of the following shall be employed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records.
 - (1) The establishment and practice of an appropriate information security management system including security risk assessment and mitigation;
 - (2) The equivalent procedures and controls that would be employed by those who are responsible for the content of electronic records;
 - (3) Additional measures such as data encryption and use of digital signature standards