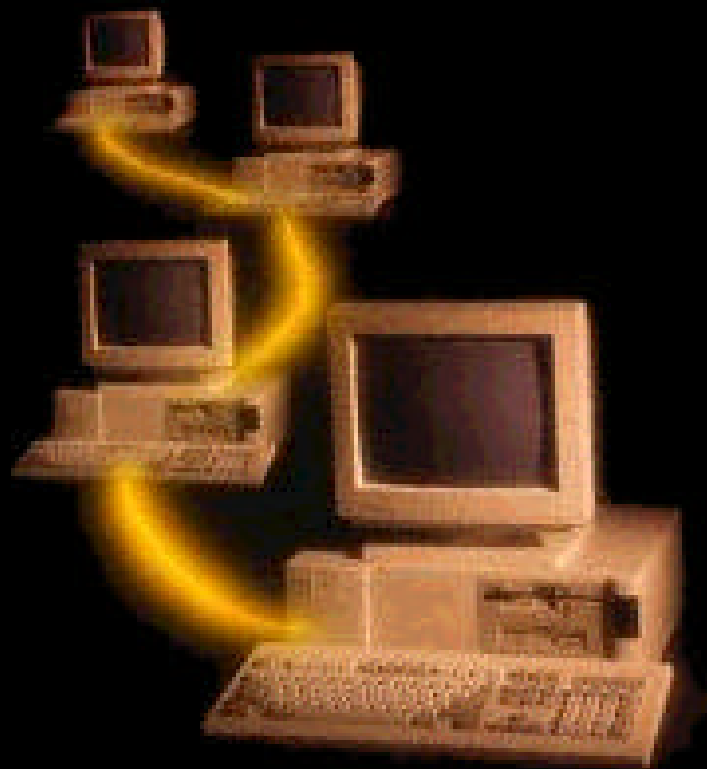


Associazionismo e Cooperazione in Medicina Generale

Convegno nazionale Co.S.

Abano Terme (PD) 31 maggio – 2 giugno 2001



Forme Associative e networking nelle Cure Primarie

Dott. Marco Visconti – Referente Co.S. per l'Informatica

La condivisione in rete degli archivi

non è solo un livello evolutivo
naturale nell'utilizzo dello
strumento informatico

ma

un presupposto indispensabile
per l'Associazione in
Medicina Generale

I bisogni

Nella quotidiana attività ambulatoriale

- in tempo reale
- senza uscire dalla cartella clinica

utilizzando standard tecnologici diffusi universalmente,

- senza ricorrere a software esterni,
- senza acquistare dotazioni hardware aggiuntive
(oltre ai necessari componenti di una rete "vera" ed efficiente)

poter interagire con gli archivi-pazienti di altri colleghi

- sia in medicina di gruppo
(rete locale, più studi medici in unica sede)
- sia in medicina in rete
(rete geografica, studi medici tra loro distanti)

avendo sempre a disposizione dati aggiornati
nel modo più semplice e meno costoso

con la certezza di agire nel pieno rispetto delle norme
sulla tutela e sulla sicurezza dei dati

BISOGNI

OPPORTUNITA'

VINCOLI

CRITICITA'

SOLUZIONI

Le opportunità

BISOGNI

OPPORTUNITA'

VINCOLI

CRITICITA'

SOLUZIONI



**ACCORDO COLLETTIVO NAZIONALE
PER LA DISCIPLINA DEI RAPPORTI
CON I MEDICI DI MEDICINA GENERALE,
AI SENSI DELL'ART. 8 DEL DECRETO LEGISLATIVO 502/92
COME MODIFICATO
DAI DECRETI LEGISLATIVI N. 517/93 E N. 229/99**

Articolo 40

6. Le forme associative disciplinate dalla lettera a) del comma 3 sono:
- A. La medicina in associazione.
 - B. La medicina in rete.
 - C. La medicina di gruppo.

Decreto Presidente Repubblica 28 luglio 1999 n.318 Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali.

CAPO I - Principi generali

Art. 1 - Definizioni

CAPO II - Trattamento dei dati personali effettuato con strumenti elettronici o comunque automatizzati.

SEZIONE I - Trattamento dei dati personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali.

Art. 2 - Individuazione degli incaricati

SEZIONE II - Trattamento dei dati personali effettuato mediante elaboratori accessibili in rete

Art. 3 - Classificazione

Art. 4 - Codici identificativi e protezione degli elaboratori

Art. 5 - Accesso ai dati particolari

Art. 6 - Documento programmatico sulla sicurezza

Art. 7 - Reimpiego dei supporti di memorizzazione

SEZIONE III - Trattamento dei dati personali effettuato per fini esclusivamente personali

Art. 8 - Parola chiave

CAPO III - Trattamento dei dati personali con strumenti diversi da quelli elettronici o comunque automatizzati.

Art. 9 - Trattamento di dati personali

Art. 10 - Conservazione della documentazione relativa al trattamento

Le criticità informatiche

Nella progettazione e nella realizzazione di una rete per le varie forme di associazionismo medico vi sono tre punti critici:

1. Gestione condivisa degli archivi
(organizzazione logica del sistema informativo)
2. Ottimizzazione ed integrazione,
finalizzate al lavoro “ in rete”,
delle varie componenti tecniche e dei software
che gestiscono la scheda sanitaria individuale
(organizzazione informatica)
3. Rispetto delle norme di sicurezza e tutela dei dati
(organizzazione “security oriented”)

BISOGNI
OPPORTUNITA'
VINCOLI
CRITICITA'
SOLUZIONI

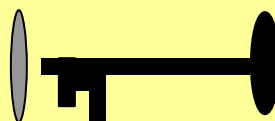
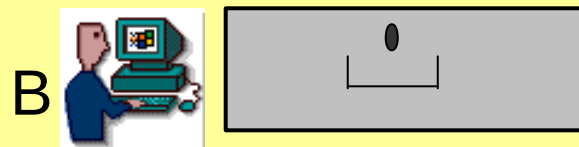
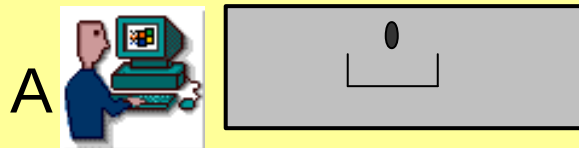
➤ Medicina di Gruppo

- con sede unica senza studi periferici
 - rete locale *peer to peer* senza server
 - rete locale con server
- con sede unica + studi periferici
 - rete locale con server + collegamenti tramite rete telefonica pubblica

➤ Medicina in Rete

- server dedicato con collegamenti tramite rete telefonica pubblica

MEDICINA DI GRUPPO con sede unica senza studi periferici
organizzazione logica 1° ipotesi: archivi in schedari separati



Ogni medico possiede, nel suo studio, uno schedario chiuso a chiave che contiene le cartelle cliniche dei suoi pazienti.

Ogni schedario si apre con una sola chiave, diversa dalle altre.

Ogni medico per aprire gli schedari degli altri deve aver ricevuto dal proprietario un duplicato della chiave.

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di Gruppo
organizzazione logica
SOLUZIONI

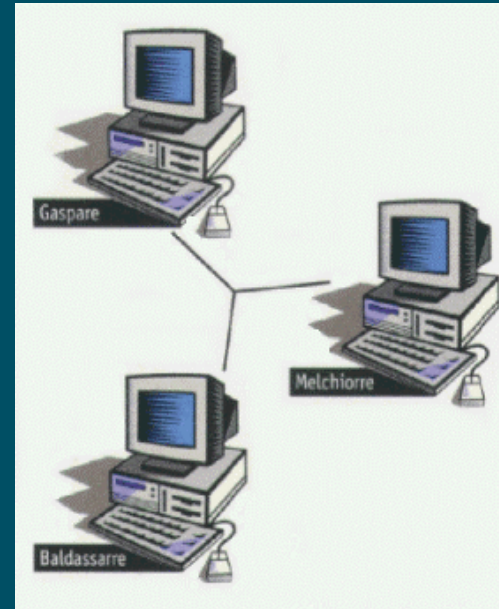
MEDICINA DI GRUPPO con sede unica senza studi periferici

organizzazione informatica 1° ipotesi: rete paritetica

Tutti medici hanno sia l'applicativo (il programma che gestisce gli archivi) sia gli archivi stessi sulla propria macchina.

Tutti i computer collegati in rete hanno la stessa importanza (da cui il termine *paritetico*) ed il collegamento avviene in modo diretto *peer to peer* tra PC e PC.

Per collegarsi all'archivio-pazienti di un altro medico del gruppo, occorre che la macchina su cui risiede sia accesa.



BISOGNI
OPPORTUNITA'
VINCOLI

Medicina di Gruppo
org.informatica

LAN paritetica
SOLUZIONI

Local
Area
Network

- Sistema economico ma poco sicuro
- Questo modello è indicato per un gruppo composto da un numero di medici di assistenza primaria più vicino a 3 che a 8.

MEDICINA DI GRUPPO con sede unica senza studi periferici **organizzazione della sicurezza 1° ipotesi: rete paritetica**

L'Amministratore di Sistema è responsabile in prima persona delle misure minime di sicurezza per ogni macchina di ogni medico (e di ogni altra figura professionale) collegata in rete. Quindi per ogni PC deve periodicamente controllare che tali misure siano attive ed efficaci, ad esempio:

- PW iniziale per utilizzare il PC (PW sul BIOS e sul S.O.)
- PW e ID per l'avvio dell'applicativo
- PW e ID di accesso ad ogni singolo archivio
- Livelli di accesso differenziati per ogni archivio (titolare del trattamento, sostituto, infermiera, altri medici del gruppo, etc etc)
- Protezione per l'accesso esterno alla cartella che contiene gli archivi-pazienti

Inoltre deve verificare per ogni macchina che:

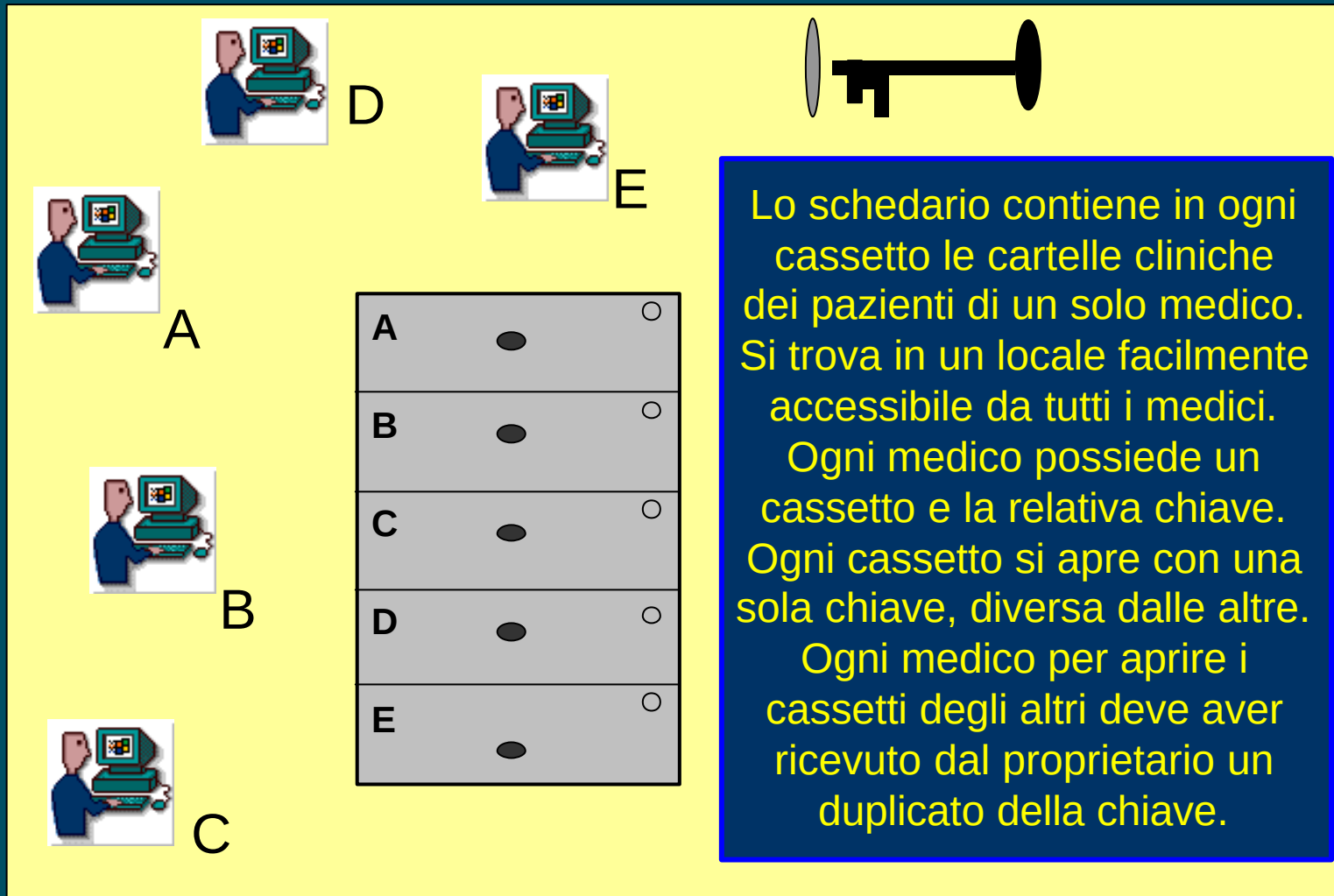
- le procedure di back up siano eseguite secondo la cadenza prevista dal Documento Programmatico Sulla Sicurezza
- il programma antivirus sia costantemente aggiornato

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di
Gruppo
Sicurezza
SOLUZIONI

Local
Area
Network

MEDICINA DI GRUPPO con sede unica senza studi periferici:
organizzazione logica 2° ipotesi: archivi in unico schedario

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di Gruppo
organizz.logica:
archivio unico
SOLUZIONI



MEDICINA DI GRUPPO con sede unica senza studi periferici

organizzazione informatica 2° ipotesi: rete LAN con server

Tutti i medici del gruppo hanno solo l'applicativo sulla propria macchina

utilizzano gli archivi-pazienti che risiedono sul server in cartelle separate (ognuna per ogni medico)

per accedere sia al proprio archivio che a quelli degli altri è sufficiente che il server sia acceso

- sistema sicuro ed affidabile
la struttura a stella (in parallelo) garantisce il funzionamento degli altri PC in caso di difetto di un elemento
- accesso veloce ai dati
- non occorre che tutti i PC siano accesi

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di Gruppo
org.informatica
LAN + server
SOLUZIONI

Local
Area
Network

MEDICINA DI GRUPPO con sede unica senza studi periferici organizzazione della sicurezza 2° ipotesi: rete LAN con server

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di
Gruppo
Sicurezza
SOLUZIONI

E' opportuno che il server sia una macchina a sé stante che non abbia altre funzioni: è da sconsigliare l'utilizzo di uno dei PC già in uso ai medici o al personale di studio come server (chi accede a quel PC di fatto ha in mano gli archivi di tutti).

A differenza dell'architettura peer to peer l'amministratore di sistema presidia solo il server dedicato e compie tutte le operazioni di verifica necessarie solo una volta.

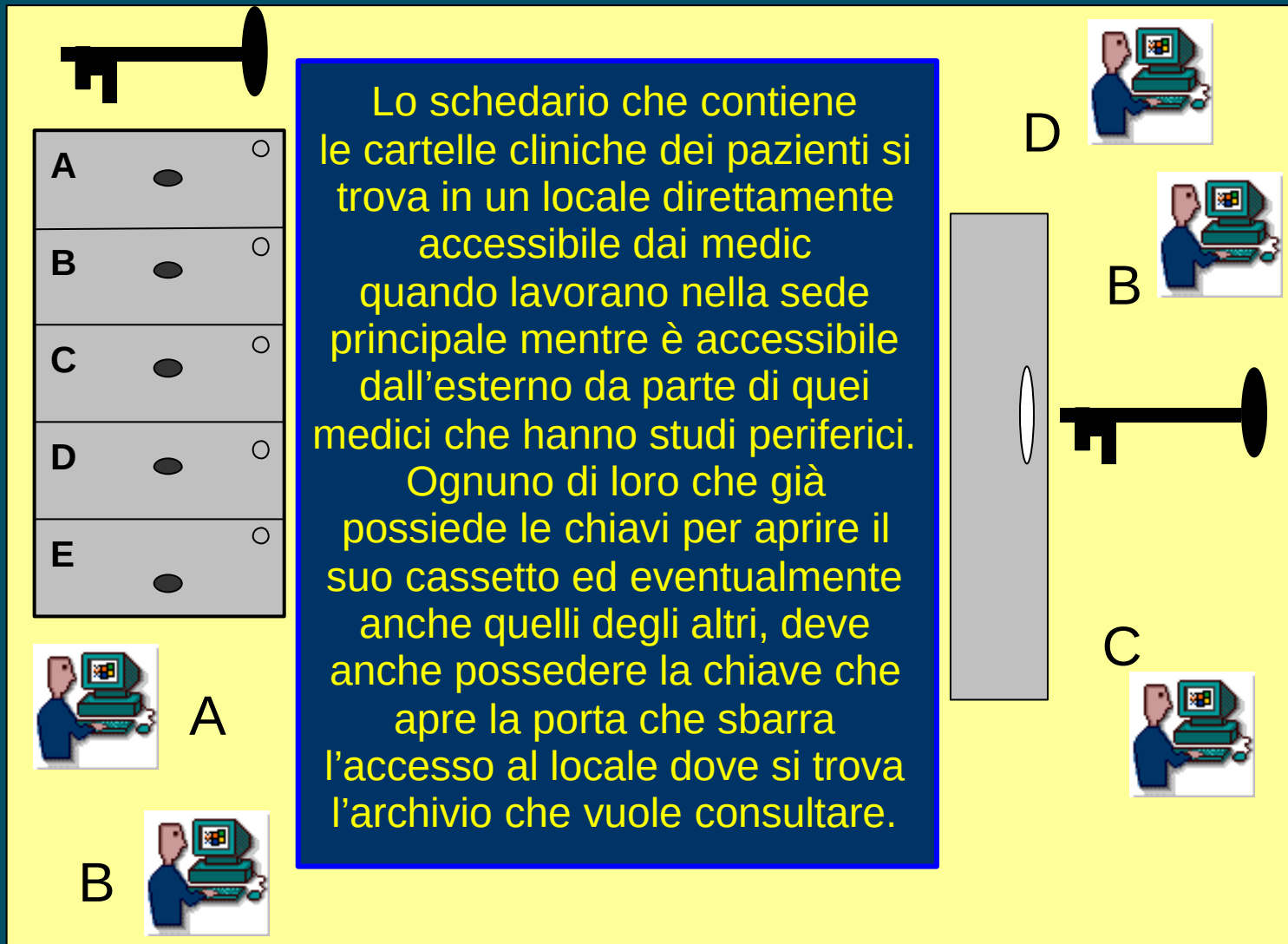
L'accesso al server è consentito solo all'Amministratore di sistema e pertanto è minimizzato il rischio di accessi impropri (dall'esterno dell'applicativo) alle cartelle contenenti gli archivi-pazienti.

inoltre:

- più facile da proteggere fisicamente (in un locale chiuso a chiave)
- più facile il controllo del backup e dell'antivirus

MEDICINA DI GRUPPO con sede unica + studi periferici
organizzazione logica
archivi in unico schedario accessibili anche dall'esterno

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di Gruppo + esterni
organizz.logica:
archivio unico
SOLUZIONI



MEDICINA DI GRUPPO con sede unica + studi periferici organizzazione informatica LAN accessibile dall'esterno

- Gli archivi-pazienti di tutti i medici risiedono sul server che si trova nella sede principale della medicina di gruppo
 - Tutti i medici quando sono nella sede principale lavorano con l'applicativo montato sulla propria macchina ed utilizzano gli archivi-pazienti che risiedono sul server locale in cartelle separate (ognuna per ogni medico).
 - Quando invece si trovano ad *“operare in altri studi del medesimo ambito territoriale ma in orari aggiuntivi a quelli previsti, nella sede principale, per l'istituto della medicina di gruppo”* lavorano con l'applicativo montato sulla propria macchina e:
 - utilizzano in locale (sulla stessa macchina) il proprio archivio-pazienti
 - utilizzano in remoto (sul server a cui si collegano mediante linea telefonica) gli archivi-pazienti degli altri medici
- L'allineamento/aggiornamento degli archivi deve avvenire in modo automatico all'inizio ed alla fine di ogni seduta di studio

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di
Gruppo + esterni
org.informatica:
archivio unico
SOLUZIONI

MEDICINA DI GRUPPO con sede unica + studi periferici

organizzazione della sicurezza

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina di
Gruppo + esterni
Sicurezza
SOLUZIONI

In aggiunta a quanto previsto per la LAN senza possibilità di accessi dall'esterno l'Amministratore di Sistema dovrà porre in atto ulteriori misure di sicurezza in quanto in questo caso il server a cui si collegano utenti esterni va annoverato tra gli *"elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico"* come previsto dall'art.3 comma b) del DPR 318/99.

In pratica il server dovrà essere gestito con un sistema operativo creato allo scopo che controlli direttamente i vari livelli d'accesso (NT, Linux, Unix) identificando e tenendo traccia di tutti coloro che si sono collegati.

Il collegamento con la linea telefonica pubblica deve avvenire

- sul versante client con modem ISDN
- sul versante server con modem ISDN + router.

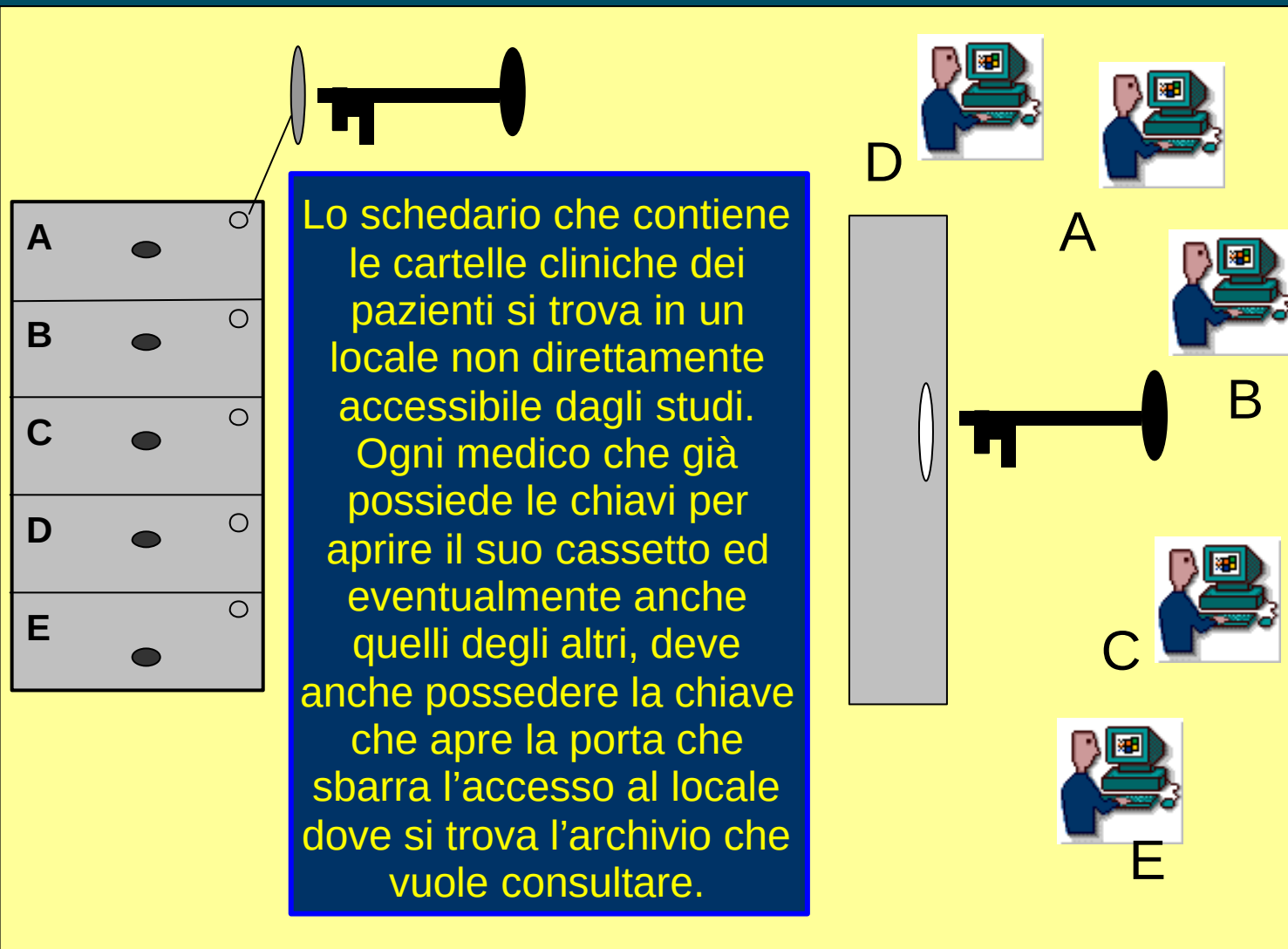
Connettersi alla rete telefonica pubblica significa infatti aprire una porta a utenti esterni, spesso non autorizzati.

Modem e Terminal Adapter non sono in grado di tutelare questa connessione da attacchi provenienti da qualsiasi altro utente.

I router, invece, garantiscono sicurezza rendendo "invisibili" all'esterno i PC locali, realizzando così un primo livello di *firewall*

MEDICINA IN RETE

organizzazione logica archivi in unico schedario remoto



BISOGNI
OPPORTUNITA'
VINCOLI
Medicina in Rete
organizz.logica:
archivio unico
SOLUZIONI

MEDICINA IN RETE

organizzazione informatica Wide Area Network (WAN)

BISOGNI
OPPORTUNITA'
VINCOLI
Medicina in Rete
org.informatica
WAN + server
SOLUZIONI

- PC collegati ad un server remoto mediante linea telefonica.
- Gli archivi-pazienti di tutti i medici risiedono sul server che si trova in una sede scelta con criteri di sicurezza e di opportunità
- Tutti i medici lavorano con l'applicativo montato sulla propria macchina ed utilizzano in remoto (sul server a cui si collegano mediante linea telefonica) gli archivi-pazienti degli altri medici.
- L'allineamento/aggiornamento degli archivi deve avvenire in modo automatico all'inizio ed alla fine di ogni seduta di studio

Questo modello è l'unico adatto a gestire in modo efficace e sicuro una rete i cui componenti siano sparsi sul territorio.

MEDICINA IN RETE

componenti di una rete WAN
(rete geografica, studi medici tra loro distanti)

BISOGNI
OPPORTUNITA'
VINCOLI
CRITICITA'
organizzazione
informatica
medicina in rete
SOLUZIONI

La costruzione di una rete "vera" ed efficiente non può prescindere da:

- un' architettura solida ed efficiente basata su:
 - tecnologie appositamente realizzate per il networking
sistemi operativi di rete per il server come (Win NT, Win 2000. Unix, Linux)
 - componenti hardware specifici



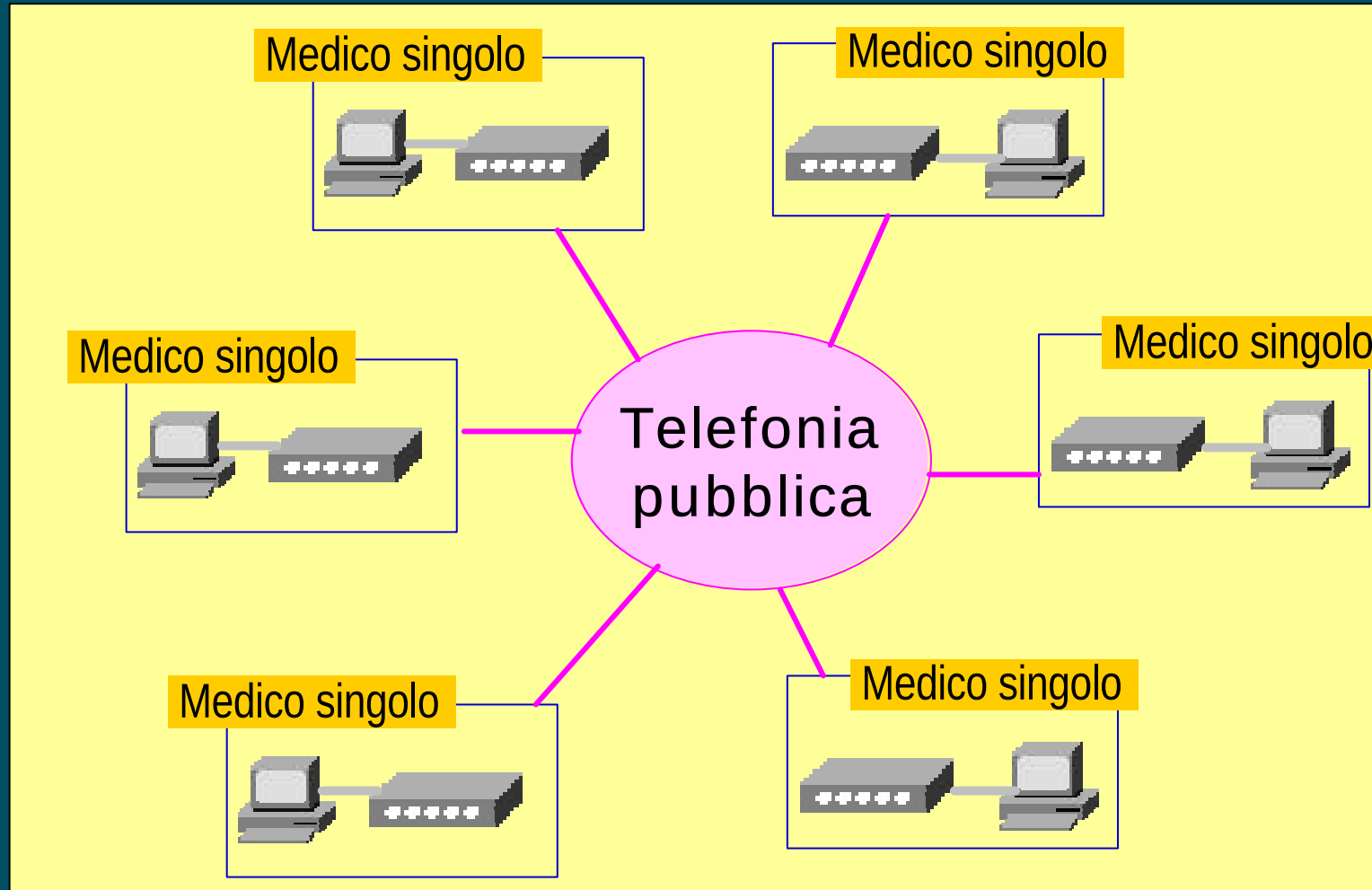
Wide
Area
Network

- protocolli di rete, di connessione e di comunicazione
universali, validi e sicuri

**Diffidate dalle improvvisazioni e/o dai surrogati !
Non utilizzate soluzioni stravaganti che non sono state progettate
per tale utilizzo e che non sono rispondenti alla *ratio* delle norme.**

Un esempio da non imitare:

condivisione di dati tra medici aventi studi in luoghi diversi, secondo una schema *point-to-point* nella quale ciascuno è in grado di accedere al computer del Collega attraverso un programma di telecontrollo.



BISOGNI
OPPORTUNITA'
VINCOLI
CRITICITA'
organizzazione
informatica
medicina in rete
SOLUZIONI

```
: 0042F785 C6403C00 mov [eax+3C], 00
: 0042F785 C6403C00 mov [eax+3C], 00
```

Tutti i sistemi di telecontrollo (tra i quali possono ricordarsi PC-Anywhere, Copycat, NetOp e Carbon Copy) sono nati per l'attività di teleassistenza, ovvero consentono di prendere il più completo controllo di tutte le risorse di un computer remoto da parte di un'amministratore di sistema

```
: 0042F7A1 E83692FFFF call 004289DC
: 0042F7A6 84C0 test al, al
: 0042F7A8 0F847A020000 je 0042FA28
: 0042F7AE 8D45F4 lea eax, dword ptr [ebp-0C]
```

Alternativamente, gli stessi sistemi possono essere utilizzati per funzioni di telesorveglianza, ovvero per verificare cosa in un dato momento stia facendo un determinato operatore di rete. Non sono stati invece concepiti per lo scambio di dati tra computer, per cui sono stati inventati, invece, i sistemi client/server, host/guest e peer-to-peer.

```
: 0042F798 0F8487020000 je 0042FA28
: 0042F7A1 E83692FFFF call 004289DC
: 0042F7A6 84C0 test al, al
```

Una regola di prudenza vorrebbe che, allorquando venisse dato accesso ad un computer remoto, l'accesso stesso possa essere limitato unicamente ai servizi strettamente indispensabili alle funzioni esperite da chi accede. Invece nello schema di telecontrollo, chi acquisisce l'accesso alla macchina ha accesso a tutte le risorse, e può fare, più o meno qualsiasi cosa.

```
: 0042F797 83784400 cmp dword ptr [eax+44], 00000000
: 0042F798 0F8487020000 je 0042FA28
: 0042F7A1 E83692FFFF call 004289DC
: 0042F7A6 84C0 test al, al
: 0042F7A8 0F847A020000 je 0042FA28
: 0042F7AE 8D45F4 lea eax, dword ptr [ebp-0C]
: 0042F7B1 B201 mov dl, 01
```

```
0042F785 C6403C00 mov [eax+3C], 00
0042F785 C6403C00 mov [eax+3C], 00
```

Nel caso in cui venga aperto un servizio di accesso ad una banca dati, si espone tale risorsa ad eventuali attacchi di chi tenta di accedervi non conoscendo la password (con tecniche che variano dal *password guessing* al *password cracking*, al *buffer overflow*)

```
0042F7A1 E83692FFFF call 004289DC
0042F7A6 84C0 test al, al
0042F7A8 0F847A020000 je 0042FA28
```

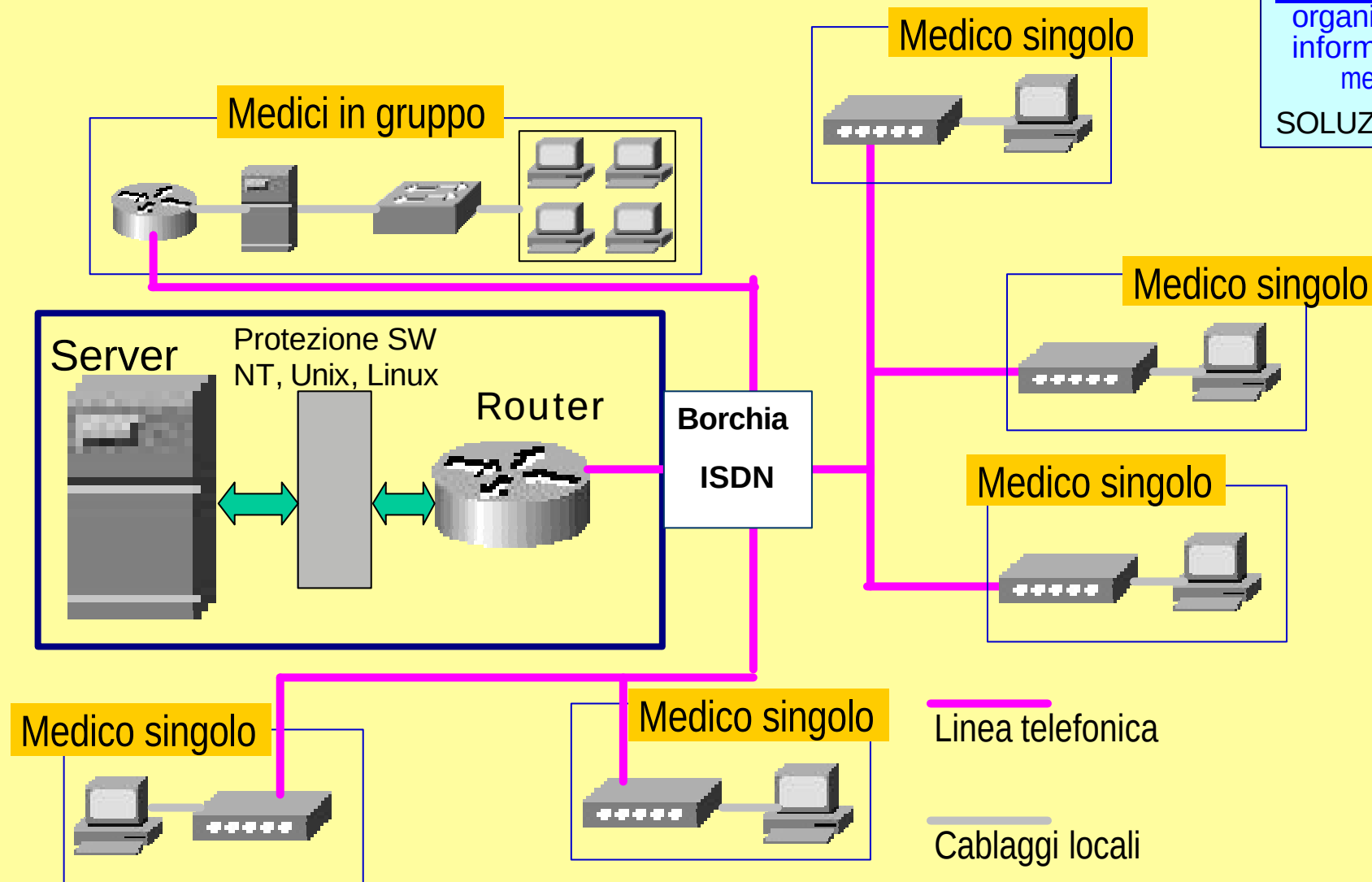
Esistono e sono facilmente reperibili programmi che non fanno altro che registrare le password immesse, scriverle in un file che poi viene inviato ad un indirizzo prestabilito, ad esempio tutte le volte che da quel computer viene inviata una posta elettronica. O ancora, è possibile ad utente anche meno smaliziato inserire un codice definito “*trojan*” che altro non fa se non imitare in tutto e per tutto un programma di telecontrollo (senza ovviamente rendersi palese), e consentire a chiunque di accedere alla macchina esattamente come se la telecontrollasse, anche se e quando venisse escluso dall’accesso mediante revoca dell’userID

```
0042F7A8 0F847A020000 je 0042FA28
0042F7AE 8D45F4 lea eax, dword ptr [ebp-0C]
```

Non è neppure possibile affermare che l’accesso tramite PC-Anywhere sia assimilabile ad un accesso ad un computer *standalone*, per cui è sufficiente avere le stesse misure di sicurezza previste per tale modalità operativa. Non v’è chi non veda infatti che la ragione per cui le misure minime per i computer standalone sono tali proprio perché è possibile escludere l’accesso alla macchina semplicemente escludendo l’accesso fisico all’apparecchiatura

MEDICINA IN RETE: architettura di una rete WAN

BISOGNI
OPPORTUNITA'
VINCOLI
CRITICITA'
organizzazione
informatica
medicina in rete
SOLUZIONI



Valgono le stesse considerazioni, in modo ancor più categorico, riportate a proposito della componente relativa agli utenti esterni di una medicina di gruppo.

Connettersi alla rete telefonica pubblica significa infatti aprire una porta a utenti esterni, spesso non autorizzati.

Pertanto i passi della sicurezza sono:

1. utilizzare per la connessione del server alla linea telefonica un router.
Modem e Terminal Adapter non sono in grado di tutelare questa connessione da attacchi provenienti da qualsiasi altro utente.
2. utilizzare i sistemi operativi di rete più volte citati che consentono la verifica e la limitazione degli accessi, tenendone oltretutto un registro
3. utilizzare un programma di gestione della cartella clinica che abbia integrate nel suo codice sorgente:
 - la procedura di connessione al server di rete
 - la verifica delle autorizzazioni per l'accesso al server di rete
 - la verifica delle autorizzazioni e l'assegnazione delle modalità di accesso

così da incanalare il flusso delle informazioni in condotte chiuse, difficilmente accessibili e scardinabili dall'esterno da parte della maggioranza degli utenti.

--- F i n e ---