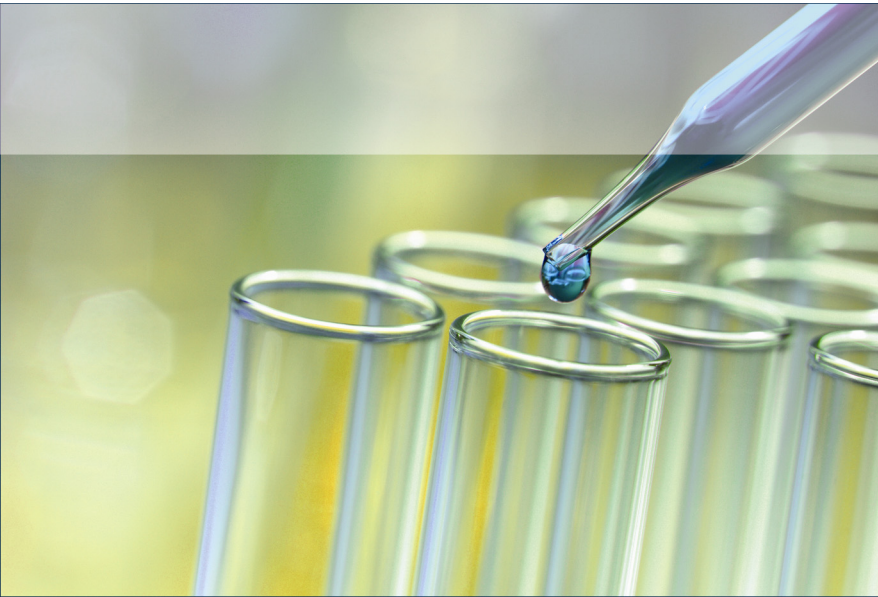




## SOLUTIONS LABORATORI DI RICERCA



### Boole Server per i Laboratori di ricerca

#### Canale di comunicazione protetto e controllato per lo scambio di file tra ricercatori

In molti ambiti dell'attività svolta all'interno dei laboratori di ricerca, i dati gestiti rappresentano delle informazioni che richiedono massima attenzione e riservatezza: per queste ragioni spesso può risultare pericoloso utilizzare sistemi vulnerabili come la posta elettronica per lo scambio di file.

Boole Server rappresenta una efficace, pratica e versatile alternativa ai tradizionali sistemi per la condivisione dei dati, poiché consente di stabilire in modo preciso e selettivo cosa condividere, con chi, per quanto tempo e secondo quali modalità.

Tutte le informazioni gestite da Boole Server sono protette e rese accessibili esclusivamente a personale autorizzato tramite specifici parametri di identificazione stabiliti di volta in volta dal responsabile di competenza.

#### Sistema per la conservazione degli esiti delle sperimentazioni nella tutela della garanzia della privacy

Qualunque laboratorio di ricerca ha il dovere, oltre che l'interesse, di garantire che tutte le informazioni relative alle sperimentazioni condotte all'interno di esso vengano conservate nel rispetto della massima discrezione.

Che si tratti di formule proprietarie, esiti di esami, dati su pazienti o di sperimentazioni terapeutiche, le informazioni archiviate in un laboratorio di ricerca richiedono di essere conservate secondo modalità che ne tutelino al massimo la riservatezza e il rispetto della privacy.

**Normativa - 16 giugno 2004**  
**A.4. CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI PER SCOPI STATISTICI E SCIENTIFICI (PROVVEDIMENTO DEL GARANTE N. 2 DEL 16 GIUGNO 2004, GAZZETTA UFFICIALE 14 AGOSTO 2004, N. 190)**

#### Art. 9. Trattamento dei dati sensibili o giudiziari

1. I dati sensibili o giudiziari trattati per scopi statistici e scientifici devono essere di regola in forma anonima.

2. Quando gli scopi statistici e scientifici, legittimi e specifici, del trattamento di dati sensibili o giudiziari non possono essere raggiunti senza l'identificazione anche temporanea degli interessati, il titolare adotta specifiche misure per mantenere separati i dati identificativi già al momento della raccolta, salvo ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato.

3. Quando i dati di cui al comma 1 sono contenuti in elenchi, registri o banche dati tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente non intelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

Per rispondere efficacemente a queste esigenze Boole Server rappresenta la soluzione attraverso cui proteggere in modo sicuro tutti i dati di cui il laboratorio è responsabile: applicando il sistema di cifratura di Boole Server infatti, solo il personale autorizzato può avere accesso al contenuto dei file archiviati.

Senza le credenziali identificative di accesso richieste, i dati protetti con Boole Server risultano indecifrabili: anche nel caso in cui i file venissero indebitamente sottratti, essi risulterebbero inutilizzabili.

### Creazione di Data Room per lo scambio di dati riservati tra laboratori di ricerca e le organizzazioni che ne gestiscono i fondi e la pubblicizzazione

Indipendentemente che facciano parte di case farmaceutiche, o strutture ospedaliere, i laboratori di ricerca possono avere necessità di scambiare informazioni proprietarie altamente riservate con organizzazioni che promuovono la loro attività.

Per fare in modo che le informazioni possano essere trasferite tempestivamente senza che ne venga compromessa la riservatezza, Boole Server consente di creare Data Room protetti e accessibili solo a personale autorizzato, in cui laboratorio ed ente esterno possono scambiarsi qualunque tipo di file in modo controllato e non intercettabile da personale non autorizzato.

#### Art. 12. Attività di controllo

1. Le università, gli altri istituti o enti di ricerca e le società scientifiche conservano la documentazione relativa ai progetti di ricerca presentati e agli impegni sottoscritti dai ricercatori ai sensi dell'art. 3, commi 1 e 2, e dell'art. 8, comma 2 del presente codice.

2. Gli enti di cui al comma 1:

a) assicurano la diffusione e il rispetto del presente codice fra tutti coloro che, all'interno o all'esterno dell'organizzazione, sono in qualunque forma coinvolti nel trattamento dei dati personali realizzato nell'ambito delle ricerche, anche adottando opportune misure sulla base dei propri statuti e regolamenti; b) segnalano al Garante le violazioni del codice di cui vengono a conoscenza.

#### Art. 15. Misure di sicurezza

1. Nell'adottare le misure di sicurezza dei dati e dei sistemi di cui agli artt. 31 e seguenti del decreto e al disciplinare tecnico contenuto nel relativo allegato B), i titolari dei trattamenti di dati per scopi statistici curano anche i livelli di accesso ai dati personali con riferimento alla natura dei dati stessi ed alle funzioni dei soggetti coinvolti nei trattamenti.

#### Art. 17. Regole di condotta

1. I responsabili e gli incaricati del trattamento che, per motivi di lavoro e ricerca, abbiano legittimo accesso ai dati personali trattati per scopi statistici e scientifici, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi definiti nel progetto di ricerca di cui all'art. 3; b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute; c) i dati personali e le notizie non disponibili al pubblico di cui si venga a conoscenza in occasione dello svolgimento dell'attività statistica o di attività ad essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui; d) il lavoro svolto è oggetto di adeguata documentazione; e) le conoscenze professionali in materia di protezione dei dati personali sono adeguate costantemente all'evoluzione delle metodologie e delle tecniche; f) la comunicazione e la diffusione dei risultati statistici sono favorite, in relazione alle esigenze conoscitive della comunità scientifica e dell'opinione pubblica, nel rispetto della disciplina sulla protezione dei dati personali; g) i comportamenti non conformi alle regole di condotta dettate dal presente codice sono immediatamente segnalati al responsabile o al titolare del trattamento.

| OBIETTIVI  | LA SOLUZIONE BOOLE SERVER   | I VANTAGGI   |
|--|---|--|
| <b>PROTEZIONE DEI DATI ARCHIVIATI</b>  | CONSERVAZIONE DEI DATI CON CIFRATURA A 2048 BIT   | I DATI ARCHIVIATI SONO INACCESSIBILI ANCHE IN CASO DI FURTO DELLE UNITÀ FISICHE DI STORAGE   |
| <b>SCAMBIO CONTROLLATO DI INFORMAZIONI</b>   | TRASFERIMENTO DEI DATI CON CIFRATURA A 2048 BIT   | I DATI TRASFERITI ANCHE SE VENISSERO INTERCETTATI RISULTEREBBERO INUTILIZZABILI  |
| <b>TRATTAMENTO DEI DATI NEL RISPETTO DELLA LEGGE PER LA TUTELA DELLA PRIVACY</b>         | SOLO IL PERSONALE AUTORIZZATO PUÒ DISPORRE DEI DATI SECONDO LE SPECIFICHE MODALITÀ CHE GLI SONO STATE CONCESSE  | ADEGUATA APPLICAZIONE DELLA LEGGE PER IL TRATTAMENTO DEI DATI  |
| <b>ADATTABILITÀ A SISTEMI GIÀ ESISTENTI</b>  | CREAZIONE SISTEMA CUSTOMIZZATO IN GRADO DI INTERFACCIARE LE PROPRIETÀ DELLA PIATTAFORMA BOOLE SERVER CON QUALUNQUE SISTEMA DI ARCHIVIAZIONE GIÀ ESISTENTE   | INTEGRAZIONE DEI SISTEMI DI SICUREZZA BOOLE SERVER SENZA NECESSITÀ DI MODIFICARE LE PROCEDURE DI LAVORO IN USO   |
| <b>CONTROLLO DELLE AUTORIZZAZIONI NELL'ACCESSO AI FILE</b>                               | PER OGNI SINGOLO FILE È POSSIBILE DECIDERE A CHI POTRÀ ESSERE DISPONIBILE, PER QUANTO TEMPO E SECONDO QUALI MODALITÀ  | VERSATILITÀ NELLA REGOLAZIONE DELLE RESTRIZIONI DI ACCESSO AI DATI   |
| <b>PROTEZIONE DELLA RISERVATEZZA ANCHE PER COLLEGAMENTI CLIENT DA REMOTO</b>             | PER AUTORIZZARE IL COLLEGAMENTO DA REMOTO È POSSIBILE ASSOCIARE A CIASCUN USERNAME NON SOLO UNA PASSWORD MA PERSINO GLI INDIRIZZI IP DA CUI È CONCESSO IL COLLEGAMENTO  | SICUREZZA E AFFIDABILITÀ NELLA FASE DI AUTENTICAZIONE PER L'ACCESSO AL SISTEMA   |
| <b>CONTROLLO DELLE OPERAZIONI EFFETTUATE DAI DIPENDENTI SUI FILE A CUI HANNO ACCESSO</b> | SISTEMA DI AUDITING ATTRAVERSO CUI CONSULTARE IL TRACCIAMENTO DI TUTTO CIÒ CHE AVVIENE ALL'INTERNO DELLA RETE BOOLE SERVER: ACCESSI, OPERAZIONI SUI FILE, CREAZIONE PROFILI   | PRATICITÀ E IMMEDIATEZZA NELLA CONSULTAZIONE DELLA REPORTISTICA RELATIVA ALLE ATTIVITÀ SVOLTE IN RETE  |
| <b>CREAZIONE ACCESSI TEMPORANEI</b>  | POSSIBILITÀ DI ASSEGNARE A CIASCUN UTENTE DELLE PRECISE FASCE ORARIE DURANTE LE QUALI AUTORIZZARLO AL COLLEGAMENTO CON IL SISTEMA<br>POSSIBILITÀ DI CONCEDERE L'ACCESSO AI SINGOLI FILE SECONDO LE MODALITÀ STABILITE DAL RESPONSABILE DEI DATI | CAPILLARE CONTROLLO DELLE AUTORIZZAZIONI PER L'ACCESSO AI FILE<br>POSSIBILITÀ DI STABILIRE PER OGNI FILE PRIVILEGI DI ACCESSO DIFFERENZIATI IN FUNZIONE DEL SINGOLO UTENTE A CUI VENGONO CONCESSI          |
| <b>SISTEMA DI AUTENTICAZIONE CONTROLLATO</b>   | CREAZIONE DI DATABASE PER L'ASSEGNAZIONE DI PASSWORD TEMPORANEE<br>RESTRIZIONI SUL NUMERO DI TENTATIVI DI ACCESSO CONSENTITI ALL'UTENTE   | PROTEZIONE DA TENTATIVI DI ACCESSO FRAUDOLENTI   |
| <b>DIFFERENZIAMENTO DELLE FUNZIONALITÀ MESSE A DISPOSIZIONE DEGLI UTENTI</b>             | PER OGNI SINGOLO UTENTE È POSSIBILE STABILIRE DELLE PRECISE E DIFFERENZIATE RESTRIZIONI FUNZIONALI  | GESTIONE PRECISA E DIFFERENZIATA DELLE OPERAZIONI CHE GLI UTENTI SONO AUTORIZZATI AD EFFETTUARE SUI FILE A CUI HANNO ACCESSO: AD ES. SOLA LETTURA O DOWNLOAD O MODIFICA                                    |
| <b>TUTELA DELLA PROPRIETÀ INTELLETTUALE</b>  | IMPOSSIBILITÀ DI EFFETTUARE LA COPIA O IL DOWNLOAD DEI FILE SU CUI È STATA APPLICATA LA PROTEZIONE<br>APPLICAZIONE DI WATERMARK ALLE ANTEPRIME DEI FILE CONDIVISI.<br>BLOCCO DEL COMANDO PRINT SCREEN   | I DATI STRATEGICI O RISERVATI SONO PROTETTI E INUTILIZZABILI IN CASO DI SOTTRAZIONE INDEBITA<br>I FILE PROTETTI NON POSSONO ESSERE COPIATI SU SUPPORTI DI MEMORIA ESTERNI (CHIAVI USB, CD, DVD, IPOD ETC.) |
| <b>GARANZIA DI BUSINESS CONTINUITY</b>   | CONFIGURAZIONE SISTEMI DI MIRRORING E LOAD BALANCE  | EFFICIENZA OPERATIVA ANCHE IN CASO DI GUASTI O MALFUNZIONAMENTI DEL SISTEMA  |
| <b>DIFFERENZIAMENTO TRA GRUPPI DI LAVORO</b>   | CAPILLARE CONFIGURAZIONE DELLE AUTORIZZAZIONI PER L'ACCESSO AI FILE E DELLE CONCESSIONI DI PRIVILEGI FUNZIONALI   | CLASSIFICAZIONE DEI FILE E DEGLI ACCESSI AUTORIZZATI SU DI ESSI  |
| <b>ADOZIONE DI UN SISTEMA DI ARCHIVIAZIONE CHE POSSA SOSTITUIRE QUELLO CARTACEO</b>      | CONSERVAZIONE DEI DATI SECONDO I REQUISITI RICHIESTI DALLA LEGGE ATTUALMENTE IN DISCUSSIONE PER L'ARCHIVIAZIONE SOSTITUTIVA DEI DOCUMENTI   | ADOZIONE DI UN SISTEMA DI ARCHIVIAZIONE CHE ANTICIPI I FUTURI REQUISITI NECESSARI PER LA VALIDITÀ DELLE DOCUMENTAZIONI DIGITALI  |

**DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 - CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

VIGENZA 27 FEBBRAIO 2004 - CONSOLIDATO CON LA LEGGE 26 FEBBRAIO 2004, N. 45 DI CONVERSIONE CON MODIFICHE DELL'ART. 3 DEL D.L. 24 DICEMBRE 2003, N. 354.

**CAPO I - MISURE DI SICUREZZA**

**Art. 31. Obblighi di sicurezza**

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

**Art. 32. Particolari titolari**

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

**CAPO II - MISURE MINIME DI SICUREZZA**

**Art. 33. Misure minime**

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

**Art. 34. Trattamenti con strumenti elettronici**

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) autenticazione informatica;
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e ad determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

**Art. 35. Trattamenti senza l'ausilio di strumenti elettronici**

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- b) previsione di procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

**Art. 36. Adeguamento**

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.