AGENZIA WEB MONZA / GUIDA 02

Sicurezza del sito professionale

Aree riservate, documenti, accessi e comunicazioni: come progettare la sicurezza delle informazioni professionali.

Documento informativo e commerciale • Ottobre 2026

Non costituisce preventivo né documento contrattuale.

La riservatezza è parte del servizio

Uno studio professionale può trattare dati di contatto, pratiche, documenti fiscali, contratti, informazioni sanitarie o altri contenuti riservati. Non tutte queste informazioni devono necessariamente transitare dal sito: il primo controllo di sicurezza consiste nel comprendere quali dati siano realmente necessari e quali strumenti siano adeguati.

Quattro livelli di protezione

- Connessioni HTTPS/TLS per proteggere i dati in transito.
- Autenticazione e autorizzazione per delimitare gli accessi agli utenti e agli amministratori.
- Protezione applicativa e dell’infrastruttura, aggiornamenti e gestione delle vulnerabilità.
- Procedure per backup, ripristino e risposta agli incidenti, commisurate al rischio.

Gli strumenti di protezione non rendono un sistema invulnerabile. La sicurezza dipende anche da configurazione, manutenzione, personale autorizzato e procedure operative.

Un certificato HTTPS non basta, da solo, a rendere sicura un’area clienti o a proteggere un database.

Area riservata e controllo degli accessi

Autenticazione

Gli accessi richiedono credenziali gestite correttamente; per profili sensibili può essere appropriata l’autenticazione multifattore. Password e sessioni devono seguire pratiche aggiornate, con possibilità di revocare accessi non più necessari.

Autorizzazioni

Ogni utente deve poter consultare solo le informazioni di sua competenza. Un assistito non deve visualizzare i documenti di un altro; un collaboratore non deve ottenere privilegi amministrativi solo perché possiede un account.

Ruoli e tracciabilità

Le funzioni riservate possono richiedere ruoli distinti per clienti, collaboratori e amministratori, con registrazione degli eventi rilevanti e attenzione alla minimizzazione dei dati nei log.

Upload e download documentali

I file caricati devono essere sottoposti a controlli su tipologia, dimensione, permessi e memorizzazione. I download riservati vanno autorizzati sul server: un semplice URL difficile da indovinare non costituisce una protezione adeguata.

Per uno studio medico o legale la progettazione dell’area riservata richiede un’analisi specifica dei dati e dei rischi.

Comunicazioni e infrastruttura

Messaggi e documenti riservati

Una chat integrata nel sito non è automaticamente adatta alla gestione di ricette, referti o pratiche riservate. Servono verifiche su destinatari, accessi, conservazione, responsabilità e misure di sicurezza. Per alcuni trattamenti possono essere preferibili servizi specializzati.

Cloudflare e protezione del traffico

Quando compatibile con il progetto, soluzioni Cloudflare possono contribuire a filtrare richieste sospette e mitigare alcune tipologie di attacchi. Non sostituiscono l’autorizzazione applicativa, la sicurezza del database o un sistema di backup.

Hosting e aggiornamenti

L’hosting è intestato al cliente. La piattaforma va dimensionata anche in funzione della gestione delle patch, delle dipendenze e delle procedure di ripristino. Le responsabilità operative vengono definite in base ai servizi effettivamente concordati.

Backup

Un backup è utile soltanto se è protetto, recuperabile e periodicamente verificato. Frequenza, retention, cifratura e localizzazione dipendono dai requisiti del progetto.

Proteggere un sistema significa anche poter reagire correttamente quando si verifica un problema.

Privacy e responsabilità: chiarezza prima di tutto

Il GDPR richiede che il trattamento dei dati personali sia valutato rispetto a finalità, basi giuridiche, minimizzazione, conservazione, rapporti con i fornitori e misure tecniche e organizzative. Per i dati relativi alla salute possono applicarsi cautele e requisiti ulteriori.

Cosa viene definito in analisi

- Quali categorie di dati transitano dal sito e chi vi accede.
- Dove vengono conservate le informazioni e quali fornitori intervengono.
- Quali ruoli privacy spettano allo studio e ai fornitori, secondo la situazione concreta.
- Quali misure di sicurezza e di conservazione sono proporzionate al rischio.
- Come vengono gestiti revoca degli accessi, esportazione e cancellazione quando dovute.

Agenzia Web Monza può progettare e implementare gli aspetti tecnici previsti; la valutazione completa della conformità organizzativa e giuridica richiede il coinvolgimento dei responsabili del trattamento e, se necessario, di professionisti competenti.

La protezione dei dati non è un prodotto standard universale: dipende dai dati, dalle persone e dalle funzioni realmente utilizzate.

Guida informativa e commerciale, priva di valore contrattuale. Le misure concretamente incluse sono definite nel progetto approvato.