Dipartimento Tecnologie Informatiche e Tecnologie Sanitarie

# Scheda check di compliance sicurezza e privacy applicativi software

AZIENDA FRUITRICE _____

| | |
|---|---|
| Denominazione software | |
| Fornitore | |
| Descrizione sintetica attività gestita | |
| Tecnologia | |
| Base dati | |

**Tabella 1 – Compliance del software**

| | Si | No |
|---|---|---|
| **1. Tipologie dei dato gestito** | | |
| - Il software gestisce dati Personali | | |
| - Il software gestisce dati Sensibili | | |
| - Il software gestisce dati Giudiziari | | |
| - Il software gestisce dati a maggior tutela | | |
| **2. Ambito di gestione del dato** | | |
| - Sono gestiti dati relativi a episodi di cura | | |
| - Sono gestiti dati relativi a cittadini | | |
| - Sono gestiti dati relativi a dipendenti | | |
| - Sono gestiti dati relativi a fornitori | | |
| **3. Rispetto delle misure minime di cui al D. Lgs. 196/03, Titolo V, capo II, "Misure minime di sicurezza"** | | |
| Il software consente l'integrazione con sistemi di sicurezza permettendo la conformità alle misure dell'allegato B del codice della privacy necessarie per lo scenario d'impiego cui è destinato. | | |
| Oppure: Il software consente una parziale integrazione con sistemi di sicurezza. Tuttavia è possibile sviluppare dei controlli compensativi che permettono la conformità alle misure dell'allegato B del codice della privacy necessarie per lo scenario di impiego cui è destinato | | |
| - La componente privata delle credenziali di accesso è di almeno 8 caratteri | | |
| - E' prevista l'obbligatorietà del cambio password al primo accesso | | |
| - E' prevista la modifica obbligatoria della password ogni 3 / 6 mesi | | |
| - E' prevista la disattivazione automatica della password dopo 6 mesi di non utilizzo | | |
| - E' prevista la disconnessione dell'utente in caso di non uso dell'applicativo per un periodo di tempo parametrizzabile | | |
| | | |
| **4. Rispetto delle misure e degli accorgimenti in tema di amministratori di sistema** | | |
| - E' prevista la possibilità di creare livelli differenziati di amministrazione del sistema | | |
| - E' previsto un sistema di registrazione (access log) per gli accessi logici degli amministratori di sistema al database di supporto dell'applicativo | | |
| - Il sistema di access log ha caratteristiche di inalterabilità, completezza e di verifica della integrità dello stesso | | |
| - L'access log contiene almeno i riferimenti temporali, la descrizione dell'evento che le ha generate, l'identificazione del soggetto che ha compiuto l'accesso | | |
| - L'access log è conservato online per almeno sei mesi | | |
| | | |

| | | |
|---|---|---|
| **5. Misure specifiche per i dati sensibili e giudiziari (se non gestiti segnare una X sul NO) -->** | | |
| - I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente dagli altri dati personali soggetti a trattamenti che non richiedono il loro utilizzo | | |
| - Sono registrati nel sistema documenti che contengono in modo non divisibile dati personali e dati sensibili riferiti all'interessato | | |
| - Il software consente l'adozione di tecniche di cifratura o di codici identificativi in relazione alla gestione di dati idonei a rivelare lo stato di salute o la vita sessuale. | | |
| - I dati sensibili o giudiziari sono trattati con tecniche di cifratura | | |
| - I dati sensibili o giudiziari sono trattati mediante codici identificativi | | |
| - I dati sensibili o giudiziari sono trattati mediante altre soluzioni rispetto alle due precedenti, ai fini della loro temporanea inintelligibilità | | |
| | | |
| **6. Funzione di repository sanitario (se non ha questa funzione segnare una X sul NO) ------->** | | |
| - Il sistema consente di rilevare e tenere traccia temporalmente dei consensi e delle cessazioni di consenso, del paziente alla attivazione del suo FSE/DSE | | |
| - Il sistema consente il collegamento con sistemi esterni per acquisire l'esistenza o meno del consenso del paziente alla attivazione del suo FSE/DSE | | |
| - Il sistema consente l'accesso al FSE/DSE solo in relazione alla preventiva definizione del mandato assistenziale attivo (visita, ricovero, ecc. ) che ne giustifica l'utilizzo | | |
| - Il sistema consente di qualificare ogni singolo episodio di cura nello status deciso dal paziente relativamente al FSE/DSE (visibile, oscurato, oscuramento dell'oscuramento) | | |
| - Relativamente ai dati a maggior tutela, il sistema consente di identificarli e di rilevare lo specifico consenso del paziente ai fini del trattamento FSE/DSE | | |
| - Il sistema consente la visibilità dei dati alla sola struttura di appartenenza del sanitario in caso di non attivazione del FSE/DSE | | |
| - Il sistema tiene traccia degli accessi al FSE/DSE, rilevando i dati dell'operatore sanitario, della postazione di lavoro di accesso, della data e ora di accesso e delle azioni, anche di sola inquiry eseguite | | |
| - Il sistema consente l'accesso al sistema da parte del paziente tramite tessera sanitaria, al fine di operare sul proprio FSE/DSE, e di verificare chi ha effettuato accessi al proprio FSE/DSE | | |

**Tabella 2. Valutazione impatto**

| **ANALISI DEL RI*SCHIO PER MANCATO FUNZIONAMENTO DEL SERVIZIO*** | |
|---|---|
| **Contesto** | **Livello di criticità** |
| Violazione di leggi, regolamenti o contratti | |
| Violazione della privacy sui dati personali | |
| Danni a persone | |
| Blocco o ritardo nella erogazione di servizi aziendali o istituzionali | |
| Effetti negativi nei rapporti con terze parti e danni all'immagine | |
| Conseguenze finanziarie | |
| | |
| VALUTAZIONE DI SINTESI | **Molto Alta** |

Criticità: **Moderata** -> Il danno è limitato

Criticità: **Alta** -> Il danno è considerevole

Criticità: **Molto alta** -> Il danno non è sostenibile

| MISURE IDONEE E REQUISITI DI SICUREZZA DA IMPLEMENTARE PER IL DISPIEGAMENTO | | |
|---|---|---|
| **PROPRIETA'** | **RICHIESTE** | **REALIZZATE** |
| Riservatezza | | |
| | | |
| | | |
| | | |
| Integrità | | |
| | | |
| | | |
| | | |
| Disponibilità | | |
| | | |
| | | |
| | | |

Data compilazione

Il compilatore