



## Conformità GDPR di 2WIN-S e 2WIN-S Plus

In Adaptica abbiamo a cuore i dati. Proteggiamo i vostri dati e quelli dei vostri clienti.

Questo documento illustra le caratteristiche di privacy e sicurezza di 2WIN e 2WIN-S Plus e fornisce suggerimenti su come migliorare ulteriormente la sicurezza dei dati.

### Caratteristiche di sicurezza di 2WIN-S e 2WIN-S Plus

2WIN-S e 2WIN-S Plus sono entrambi composti da una fotocamera di screening visivo 2WIN, un tubo Kaleidos e un tablet di controllo con l'App KALEIDOS BT. Queste sono le caratteristiche e le specifiche relative alla sicurezza dei dati memorizzati nei due dispositivi.

- Il 2WIN-S esegue solo esami anonimi, quindi nessun dato personale viene memorizzato nel dispositivo.
- Nell'App KALEIDOS BT è possibile inserire i dati del paziente (disponibile dalla versione software 5.4). Questi dati non vengono inviati al 2WIN-S e sono conservati all'interno del tablet di controllo.
- KALEIDOS App BT funziona solo se nel tablet di controllo è stato impostato un blocco di sicurezza. L'applicazione avvisa l'utente se il blocco di sicurezza non è impostato e non si avvia finché non viene impostato.
- L'applicazione AI (disponibile dalla versione software 5.5.0) invia e memorizza solo dati anonimi e la quantità minima necessaria per l'assistenza, se necessario.
- L'integrazione con l'EMR (disponibile dalla versione software 5.5.0) richiede che l'utente imposti una cartella condivisa. Questa operazione deve essere eseguita con il protocollo samba e richiede l'impostazione di una password sulla cartella condivisa.
- Nella cartella condivisa viene salvato un solo esame alla volta, in modo da evitare esami multipli non controllati direttamente dall'applicazione.

### Suggerimenti per migliorare la sicurezza

Al fine di migliorare la sicurezza dei dati, si raccomanda vivamente di intraprendere le seguenti azioni.

1. Crittografare il tablet di controllo con un ID o una password sicuri.  
2WIN-S Plus viene fornito con una console remota dedicata (tablet), già crittografata con una password predefinita. Tuttavia, vorremmo che foste voi a impostare la vostra password, in modo che solo voi possiate accedere ai vostri dati. In caso di furto del dispositivo, questo impedirebbe a estranei di accedere ai dati contenuti.  
Scegliete un blocco dello schermo di sicurezza adeguato, ad esempio un ID con almeno 6 numeri o una password di almeno 8 caratteri che includa lettere maiuscole, numeri e simboli.
2. Lo stesso consiglio per la password vale per proteggere la cartella condivisa dell'EMR.
3. Per proteggere la cartella condivisa EMR, aggiornare regolarmente il PC o il server da cui è impostata la cartella condivisa con le ultime patch di sicurezza del sistema operativo.