



Conformidade do GDPR de 2WIN-S e 2WIN-S Plus

Em Adaptica nos preocupamos com os dados. Protegemos seus dados e os dados de seus clientes. Este documento explica as características de privacidade e segurança do 2WIN e 2WIN-S Plus e dá dicas sobre como melhorar ainda mais a segurança dos dados.

Características de segurança 2WIN-S e 2WIN-S Plus

O 2WIN-S e o 2WIN-S Plus são ambos compostos por uma câmera de triagem visual 2WIN, um tubo Kaleidos e um tablete de controle rodando o KALEIDOS App BT. Estas são as características e especificações relativas à segurança dos dados armazenados nos dois dispositivos.

- O 2WIN-S realiza apenas exames anônimos, de modo que nenhum dado pessoal é armazenado no dispositivo.
- No KALEIDOS App BT é possível inserir dados do paciente (disponível a partir da versão de software 5.4). Estes dados não são enviados para o 2WIN-S e são mantidos dentro da placa de controle.
- O KALEIDOS App BT só funcionará se for instalado um cadeado de segurança no tablete de controle. O aplicativo avisará o usuário se a trava de segurança não estiver configurada e não iniciará a operação até que esta esteja configurada.
- O aplicativo AI (disponível na versão 5.5.0 do software) envia e armazena apenas dados anônimos e a quantidade mínima necessária para o serviço, se necessário.
- A integração EMR (disponível a partir da versão de software 5.5.0) requer que o usuário crie uma pasta compartilhada. Isto deve ser feito com o protocolo samba e requer que uma senha seja configurada na pasta compartilhada.
- Apenas um exame por vez é salvo na pasta compartilhada, a fim de evitar vários exames que não estejam sob controle direto da aplicação.

Dicas para melhorar a segurança

A fim de melhorar a segurança dos dados, as seguintes ações são fortemente recomendadas.

1. Encripte seu tablet de controle com uma identificação ou senha segura.
2WIN-S Plus vem com um Console remoto dedicado (tablet), que já está criptografado com uma senha padrão. Mas gostaríamos que você criasse sua própria senha, para que somente você possa acessar seus dados. Caso o dispositivo seja roubado, isto impediria que estranhos acessassem os dados dentro dele.
Escolha um cadeado de segurança adequado, como uma identificação com pelo menos 6 números ou uma senha de pelo menos 8 caracteres, incluindo números e símbolos em maiúsculas.
2. O mesmo conselho para a senha é verdadeiro para proteger a pasta compartilhada da EMR.
3. Para proteger a pasta compartilhada EMR, atualize regularmente o PC ou servidor a partir do qual a pasta compartilhada é configurada com os últimos patches de segurança do sistema operacional.