eCRF Medicalcouncil: Standard di protezione del dato elettronico

Scopo del documento

Lo scopo del documento è di illustrare come le linee guida per la sicurezza del dato elettronico richieste dallo standard FDA CRF21 part 11 sono state implementate all'interno dell'applicazione eCRF sviluppata dalla Medicalcouncil s.r.l. . L'applicazione è basata sulla struttura web e rispetta a tutte le linee guida dello standard FDA CRF21 part 11.

Autenticazione degli utenti

Lo standard FDA richiede misure di sicurezza per prevenire accessi non autorizzati ai dati. Per prevenire gli accessi non autorizzati nell'applicazione è stato implementato un sistema di autenticazione forte: Per ogni utente è prevista un username univoco e una password. La password deve avere lunghezza minima di 8 caratteri ed ha validità 60 giorni. Allo scadere dei 60 giorni viene chiesto all'utente di cambiare password. Inoltre dopo 5 tentativi consecutivi di inserimento di una password errata, o 3 tentativi di inserimento di una risposta alla domanda di sicurezza errata l'utente viene bloccato.

La password viene registrata sul database con crittografia unidirezionale SHA-512. Prima della codifica alla password viene aggiunta una stringa casuale generata per ogni utente di lunghezza 6 caratteri. La password codificata risultante da queste operazioni è univoca anche se due utenti scelgono la stessa password.

Al primo accesso al sistema all'utente viene chiesto di modificare la password ed inserire sia una domanda di sicurezza che una risposta alla stessa. La risposta alla domanda di sicurezza viene salvata sulla base dati con gli stessi criteri della password.

La sessione di lavoro scade automaticamente dopo 20 minuti di inattività per prevenire che personale non autorizzato possa sostituirsi al terminale al posto del medico.

Firma digitale

Per il profilo dei medici, gli unici autorizzati ad inserire e modificare i dati contenuti nel sistema, viene generata una seconda password. E' a carico della società committente consegnare la seconda password ai medici stessi. Questa seconda password viene richiesta dal sistema nel momento in cui si inseriscono o si aggiornano i dati.

Audit trial

Il Sistema prevede 2 tipi di audit trial per garantire l'integrità, l'autenticità e la confidenzialità dei dati:

- Audit trial accessi: Vengono registrati dal sistema in una tabella dedicata tutti gli accessi e le uscite dallo stesso, i tentativi di accesso con user errato (accesso anonimo) e i tentativi di accesso con password o domanda di sicurezza errata.

- Audi trial dati: Vengono registrati dal sistema in una tabella dedicata tutte le modifiche e gli inserimenti dei dati. Ogni modifica o inserimento riporta l'identificativo univoco del medico che lo ha effettuato, il centro di appartenenza del medico, il numero del paziente e il numero della visita i cui dati appartengono, la data dell'operazione, l'elenco dei campi modificati o inseriti con il vecchio valore ed il nuovo, la tabella su cui sono andate ad incidere le modifiche, il numero di riga che il sistema ha scritto ed in caso di modifica il motivo per cui è stato effettuato il cambiamento.

Sicurezza dei dati nella base dati

Ogni record del database è crittografato con chiave simmetrica a 256 bit (Advanced Encryption Standard (AES)). Questo algoritmo ha la caratteristica di essere veloce e garantire ne contempo un ottima sicurezza dei dati. Lo stesso algoritmo viene usato anche dall' U.S. National Institute of Standards and Technology (NIST). La chiave necessaria per il funzionamento dell'algoritmo AES è configurata durante l'installazione del sistema.

Comunicazione client server

L'applicazione si basa su tecnologia web, quindi utilizza il sistema di comunicazione client (il browser (Firefox unico garantito) che utilizza l'utente) – server (Il server remoto dove risiede il database(Fornito da www.amazon.com)). Per garantire la sicurezza del canale di comunicazione tramite internet si utilizza il protocollo di sicurezza Transport Layer Security (TLS) che a sua volta si basa sul protocollo Secure Sockets Layer (SSL). Il protocollo TLS crittografa i le connessioni di rete a livello applicazione per il Transport Layer, utilizzando la crittografia asimmetrica per lo scambio di chiavi, la crittografia simmetrica di riservatezza, e codici di autenticazione dei messaggi per l'integrità del messaggio. Il protocollo TLS consente alle applicazioni client-server di comunicare in rete in un modo studiato per evitare interferenze e manomissioni.