Allegato D - MDS2_Italiano_v2b

DICHIARAZIONE DEL FABBRICANTE SULLA SICUREZZA DEI DISPOSITIVI MEDICI ATTIVI / IVD - SDM/IVD

Classificazione DM/IVD/IVD (Classificazione Nazionale Dispositivi Med	Fabbricante	ID Documento	Data pubblicazione documento

Modello DM/IVD/IVD	Revisione Software	Data di rilascio del software

Informazioni relative al contatto del fabbriacante o mandatario	Nome	Titolo	Divisione
	Ragione Sociale	Telefono	e-mail

	Gestione dei dati sensibili	SI/No/ N.a.	Se SI descrivere. Se NO indicare le motivazioni
A	**Possibilità da parte del DM/IVD/IVD di visualizzare, trasmettere o mantenere dati privati (inclusi dati sensibili)**		
B	**Tipologie di dati privati trattati dal DM/IVD/IVD**		
B.1	***Demografici***		
B.1.1	Nome e cognome		
B.1.2	Indirizzo		
B.1.3	Localizzazione		
B.1.4	Identificativo unico		
B.1.5	Altro		
B.2	***Dati medici***		
B.2.1	Identificativo tessera sanitaria		
B.2.2	Dati assicurazione		
B.2.3	Esame o data del trattamento		
B.2.4	Numero identificativo del DM/IVD/IVD		
B.2.5	Altro		
B.3	***Diagnostici/terapeutici***		
B.3.1	Foto/radiografie		
B.3.2	Risultati degli esami / Referti		
B.3.3	Dati fisiologici con caratteristiche identificative		
B.3.4	Altro		
B.4	***Aperto, testo non strutturato inserito dall'utilizzatore/operatore sanitario***		
C	**Memorizzazione dati sensibili**		
C.1	Conservazione dei dati sensibili temporaneamente nella memoria volatile (es. cancellata al reset o all'accensione)		
C.2	Memorizzazione dei dati sensibili in modo permanente su supporto locale		
C.3	Importazione/esportazione dati sensibili con altri sistemi		
C.4	Memorizzazione dei dati sensibili durenat einterruzioni di servizio		
D	**Sistema utilizzato dal DM/IVD/IVD per trasmettere, importare/esportare i dati sensibili.**		
D.1	Visualizzazione dei dati sensibili		
D.2	Generazione di report o immagini contenenti dati sensibil		
D.3	***Recupero di dati sensibili o registrazione di dati sensibili su supporti rimovibili***		
D.3.1	dischi		
D.3.2	DVD / BlueRay		
D.3.3	CD-ROM		
D.3.4	Nastri		
D.3.5	Carte CF/SD		
D.3.6	Memory stick		
D.3.7	Altro		
D.4	***Trasmissione/ricezione o importazione/esportazione di dati sensibili attraverso una connessione dedicata***		
D.4.1	IEEE 1073		
D.4.2	Porta seriale		
D.4.3	USB (indicare tipo)		
D.4.4	FireWire		
D.4.5	Altro		
D.5	***Trasmissione/ricezione di dati sensibili attraverso la rete***		
D.5.1	LAN		
D.5.2	WAN		
D.5.3	VPN		
D.5.4	Intranet		
D.5.5	Internet		
D.5.6	Altro		
D.6	***Trasmissione/ricezione di dati sensibili attraverso una connessione wireless integrata***		
D.6.1	WiFi		
D.6.2	Bluetooth		
D.6.3	Infrarosso (IRDA)		
D.6.4	ZigBee		
D.6.5	Altro		
D.7	Importazione di dati privati con metodi di scannerizzazione		
D.8	Altro		
	CARATTERISTICHE DI SICUREZZA		
1	**Automatic LOGOFF (ALOF)**		
1.1	***Possibilità di configurazione per forzare il log-in dell'utilizzatore dopo un periodo predeterminato di inattività***		

1.1.1	Auto logoff		
1.1.2	Session Lock		
1.1.3	Screen saver protetto da password		
1.1.4	Altro		
1.2	Possibilità di configurare da parte dell'utente/amministratore la durata del periodo di inattività prima dell'auto logoff/protezione screen saver (se SI indicare la durata se fissa o il range se configurabile)		
1.3	Possibilità di invocare manualmente da parte dell'utente l'auto logoff/protezione screen saver (se SI indicare la modalità)		
1.4	Altro (descrivere)		
2	**Audit Controls (AUDT) [La capacità del DM/IVD di registrare in modo affidabile l'attività sul DM/IVD stesso]**		
2.1	Possibilità da parte del DM/IVD di creare un registro di attività		
2.2	***Eventi registrati nell'AUDIT log***		
2.2.1	Login / Logout		
2.2.2	Visualizzazione / presentazione dei dati		
2.2.3	Creazione / modifica / cancellazione di dati		
2.2.4	Importazione / esportazione di dati da media removibili		
2.2.5	Ricezione / trasmissione di dati da/verso connessioni (rete) esterne		
2.2.5.1	Attività service remote		
2.3	***Tipologia di informazioni utilizzate per identificare gli eventi songoli registrati nell'AUDIT log***		
2.3.1	Identificazione utilizzatore (User ID)		
2.3.2	Data e ora dell'evento		
2.3.3	Altro		
3	**Autorizzazione (AUTH) La capacità del DM/IVD di determinare e gestire le autorizzazioni degli utenti]**		
3.1	Possibilità da parte del DM/IVD di prevenire accessi di utenti NON autorizzati attraverso la gestione dei dati di login o altri meccan		
3.2	Possibilità di assegnare all'utilizzatore privilegi diversi in funzione del ruolo		
3.3	Possibilità da parte del conduttore del device e/o dell'operatore di possedere privilegi di amministratore (senza restrizioni)		
3.4	Altro		
4	**Configurazione delle caratteristiche di sicurezza [possibilità di configurare/riconfigurare le caratteristiche di sicurezza in funzione delle necessità dell'utente] (CFNS)**		
4.1	Possibilità da parte dell'amministratore di configurare le caratteristiche di sicurezza del DM/IVD		
4.2	Altro		
5	**Aggiornamenti di sicurezza per Cybersecurity [La possibilità da parte dello staff on-site / remoto / autorizzato di installare/aggironare patch di sicurezza per il DM/IVD] (CSUP)**		
5.1	Possibilità di applicare patch di sicurezza del OS (Operating System) e/o del DM/IVD quando disponibili		
5.1.1.	Possibilità di installare le patch di sicurezza o altro software remotamente		
5.2	Altro		
6	**Anonimizzazione dei dati sensibili [La capacità del DM/IVD di rimuovere le informazioni che permettono l'identificazione del paziente] (DIDT)**		
6.1	Disponibilità di caratteristiche e strumenti integrati nel DM/IVD per anonimizzare i dati sensibili		
6.2	Altro		
7	**Backup dei dati e Disaster Recovery [La capacità di recuperare dopo un guasto o un grave danno al DM/IVD i dati, l'HW e/o il**		
7.1	Disponibilità di gestione backup (remoto o su media locale)		
7.2	Altro		
8	**Accesso di emergenza [La possibilità da parte degli utilizzatori di accedere ai dati sensibili in situazioni di mergenza che richieddono l'immediata conoscenza di tali dati] (EMRG)**		
8.1	Presenza sul DM/IVD di una caratteristica di accesso in emergenza ("breaking glass")		
8.2	Altro		
9	**Integrità e autenticità dei dati sensibili [Modalità con cui il DM/IVD assicura che i dati trattati non sono stati alterati o distrutti in un modo NON autorizzato e che provengano dall'entità che li ha generati] (IGAU)**		
9.1	Disponibilità di una caratteristica che assicuri l'integrità dei dati memorizzati attraverso l'uso di una tecnologia implicita od esplicita di detezione/correzione degli errori		
9.2	Altro		
10	**Detezione / Protezione da Malware [La capacità effetttiva del DM/IVD di individuare, prevenire e rimuovere software malevolo (malware)] (MLDP)**		
10.1	Il DM/IVD supporta l'uso di software anti-malware		
10.1.1	Possibilità da parte dell'utilizzatore di riconfigurare indipendentemente le caratteristiche anti-malware		
10.1.2	Interfaccia utilizzatore che supporta le notifiche della detezione di malware		
10.1.3	Possibilità SOLO da parte di personale autorizzato dal fabbricante di riparare i sistemi quando infettati da malware		
10.2	Possibilità da parte dell'amministratore di installare o aggiornar eil software anti-virus		
10.3	Possibilità da parte dell'amministratore di aggiornare le firme relative all'anti-virus installato		
10.4	Altro		
11	**Autenticazione di Nodo [La capacità del DM/IVD di autenticare nodi] (NAUT)**		
11.1	Possibilità da parte del DM/IVD di fornire / supportare qualsiasi mezzo di autenticazione del nodo che assicura che il mittente e il destinatario dei dati siano noti l'uno all'altro e siano autorizzati a ricevere le informazioni trasferite		
11.2	Altro		
12	**Autenticazione Utilizzatore [La capacità del DM/IVD di autenticare gli utilizzatori] (PAUT)**		
12.1	Possibilità da parte del DM/IVD di supportare UserName se Password Specifiche per almeno un utilizzatore		
12.1.1	Possibilità da parte del DM/IVD di supportare UserName se Password Specifiche per più utilizzatori		
12.2	Possibilità di configurare il DM/IVD per autenticare gli utilizzatori attraverso un servizio di autenticazione esterna		
12.2.1	MS Active Directory		
12.2.2	LDAP		
12.2.3	Altro		
12.3	Capacità del DM/IVD di bloccare l'accesso di un utilizzatore dopo un certo numero di tentativi con credenziali non corrette		
12.4	Possibilità di settare le password di default durante/prima dell'istallazione		
12.5	Possibilità di utilizzare identificativi condivisi all'interno del sistema		
12.6	Possibilità di forzare la creaione di password utente che rispettino regole di formazione complesse		
12.7	Configurazione delle password utente con scadenza predefinita		
12.8	Altro		

13	**Blocchi fisici [I blocchi fisici consentono di prevenire accessi da parte degli utilizzatori non autorizzati al DM/IVD che possano compromettere l'integrità e la confidenzialità dei dati memorizzati sul DM/IVD] (PLOK)**		
13.1	Tutti i componenti del DM/IVD che memorizzano dati sensibili (eccetto i MEDIA removibili) sono FISICAMENTE sicuri (non posson		
13.2	Altro		
14	**RoaDM/IVDap per componenti di terze parti presenti nel ciclo di vita del DM/IVD [Piani del fabbricante per supportare la sicurezza dei componenti di terze parti nell'ambito del ciclo di vita del DM/IVD] (RDM/IVDP)**		
14.1	Indicare su documento a parte SO/SW di terze parti e relative versioni		
14.2	Disponibilità della lista di SW di terze parti fornita dal fabbricante		
14.3	Altro		
15	**Hardening del sistema e delle applicazioni [Resistenza del DM/IVD verso i cyber attcks e il malware] (SAHD)**		
15.1	Indicare le misure di contrasto supportate (livello di conformance rispetto agli standard applicabile)		
15.2	Il DM/IVD supporta qualche meccanismo che assicur che i programmi / aggiornamenti installati sono autorizzati dal fabbricante		
15.3	Caratteristiche / possibilità di comunicazione esterna (network, modem, ecc)		
15.4	Il sistema supporta l'implementazione di controllo di accesso a livello di file (ES. NTFS PER MS)		
15.5	Accounts / applicazioni disabilitati / cancellati se non coerenti con la destinazione d'uso prevista		
15.6	Risorse condivise disabilitate se non utilizzate in coerenza con la destinazione d'uso prevista.		
15.7	Porte di comunicazione chiuse / disabilitate se non coerenti con la destinazione d'uso prevista		
15.8	Servizi (es. Telnet, IIS, FTP, ecc.) disabilitati / cancellati se non utilizzati in coerenza con la destinazione d'uso prevista		
15.9	Applicazioni (es. COTS, OS, MS Explorer, ecc.) disabilitate / cancellate se non utilizzati in coerenza con la destinazione d'uso previs		
15.10	Possibilità di avvio (boot) del DM/IVD da media removibili NON controllati		
15.11	Possibilità di installare SW o HW non autorizzati dal fabbricante del DM/IVD sul DM/IVD stesso senza l'uso di strumenti specifici		
15.12	Altro		
16	**Guida sulla Sicurezza [Disponibilità di una guida sulla sicurezza per l'utilizzatore, l'amministratore, i fornitori del sistema e dei servizi di manutenzione] (SGUD)**		
16.1	Disponibilità per l'utilizzatore di documentazione sulle caratteristiche di sicurezza del DM/IVD		
16.2	Disponibilità di specifiche istruzioni per la cancellazione permanente dei dati personali e/o sensibili		
16.3	Altro		
17	**autorizzati non compromettano l'integrità e la condifenzialità dei dati memorizzati nel DM/IVD o nei media removibili] (STCF)**		
17.1	Possibilità di crittografare i dati memorizzati		
17.2	Altro		
18	**Confidenzialità nella trasmissione [L'abilità del DM/IVD di assicurare la confidenzialità dei dati sensibili trasmessi] (TXCF)**		
18.1	Dati sensibili trasmessi solo con un cavo dedicato punto-a-punto		
18.2	Dati sensibili criptati prima della trasmissione via network o via media removibile (se Si indicare lo standard di crittografia utilizza		
18.3	Trasmissione dei dati sensibili ristretta ad una lista fissa di destinatari di rete		
18.4	Altro		
19	**Integrità nella trasmissione [L'abilità del DM/IVD di assicurare l'integrità dei dati sensibili trasmessi] (TXIG)**		
19.1	Il DM/IVD supporta modalità volte ad assicurare che i dati non sono modificati durante la trasmissione (Se SI descrivere in dettagl		
19.2	Altro		
20	**Altre considerazioni sulla Sicurezza [Ulteriori considerazioni/note relative alla sicurezza del DM/IVD] (OTHR)**		
20.1	Possibilità di manutenzione remota		
20.2	Possibilità di restrizione dell'accesso remoto		
20.2.1	Restrizione sugli utilizzatori		
20.2.2	Restrizioni sugli indirizzi di rete		
20.2.3	Altro		
20.3	Possibilità di configurare il DM/IVD per richiedere che l'utente locale accetti o avvi l'accesso remoto		
20.4	Altro		