

VADEMECUM

sulla normativa che regola
l'utilizzo dei software gestionali
e clinici per la Medicina Generale

Norme · Disposizioni · Sanzioni



Le informazioni contenute in questo Vademecum hanno finalità divulgativa e sono aggiornate a settembre 2026. Non sostituiscono i testi normativi né eventuali pareri professionali. Gli importi, gli adempimenti e le scadenze possono essere modificati da successivi provvedimenti.

VADEMECUM

sulla normativa che regola
l'utilizzo dei software gestionali
e clinici per la Medicina Generale

Norme · Disposizioni · Sanzioni

Prefazione

Gentile Dottoressa, Gentile Dottore,

abbiamo deciso di realizzare questo vademecum per aiutarla a orientarsi nel contesto, sempre più complesso, dei software e degli strumenti informatici per la Medicina Generale.

Molti non sono a conoscenza del fatto che, negli ultimi tre anni, il quadro normativo è profondamente cambiato, introducendo novità molto rilevanti in diversi ambiti: la certificazione dei software clinico-gestionali, derivante dal Regolamento Europeo CE MDR; le nuove disposizioni e l'estensione degli obblighi in materia di GDPR; le nuove regole relative ai sistemi Cloud, che devono essere compliant con le certificazioni ACN; e, infine, le nuove norme in ambito di Cybersecurity, che a breve porteranno alla piena entrata in vigore della certificazione NIS2.

A tutto questo si aggiunge la nuova frontiera dell'Artificial Intelligence che, a seguito dell'AI Act della Comunità Europea, porterà a breve all'applicazione della normativa nazionale in materia.

CE MDR, GDPR, ACN, NIS2, AIA sono sigle con le quali ogni medico deve ormai necessariamente confrontarsi, poiché si tratta di normative già in vigore e che prevedono sanzioni molto rilevanti per il Medico di Medicina Generale e il Pediatra di Libera Scelta. Le sanzioni per la non compliance CE MDR partono da 20.000 euro per medico e possono arrivare fino a 120.000 euro, come definito dalla legge 137 del 5 agosto 2022.

Come suggerito dalla FNOM-CEO in una recente comunicazione di fine luglio, che invita a verificare la compliance dei software utilizzati per evitare pesanti sanzioni, è importante andare oltre le semplici dichiarazioni di alcuni produttori che attestano compliance non reali.

È ancora più importante essere consapevoli del fatto che molte delle funzionalità presenti negli applicativi per la Medicina Generale devono essere compliant CE MDR, pena l'applicazione di sanzioni al produttore o, nei casi più gravi, al medico utilizzatore.

Il Regolamento Europeo, pienamente in vigore in Italia dal 2021 e operativo dal maggio 2024, stabilisce chiaramente che risultano a norma i prodotti che erano certificati MDR CE I prima del 25 maggio 2024 e che avevano già avviato l'iter per la certificazione MDR CE II A.

Si tratta di un percorso lungo e complesso, caratterizzato da numerosi prerequisiti e articolato in oltre 17 step di approvazione, che richiede inoltre la sottoscrizione, entro settembre 2024, del contratto con l'Ente Notificato incaricato del rilascio della certificazione.

Le Software House che non hanno seguito questo iter e che continuano a vendere e mantenere software contenenti funzioni

rientranti nelle Classi 2X risultano invece fuori norma dal maggio 2024.

Oggi possono essere utilizzati senza rischi solo prodotti pienamente in regola. In ogni caso, se dopo il 31 dicembre 2028 anche prodotti come Millewin e Milleweb, che oggi risultano conformi, non avranno ottenuto la certificazione MDR CE 2A, anch'essi risulteranno fuori norma.

Millennium, dopo due anni e mezzo di lavoro, si trova oggi nella fase finale dell'iter, avendo completato tutti i 16 step necessari per arrivare all'ispezione conclusiva da parte dell'Ente Notificato.

È quindi importante essere pienamente consapevoli del fatto che molte delle dichiarazioni oggi presenti sul mercato non sono veritiere e che solo il rispetto del percorso sopra descritto garantisce la conformità alla normativa.

In particolare, non sono a norma i software che:

- presentano funzionalità che rientrano nella Classe MDR CE 2A, quali, ad esempio, interazioni tra farmaci, calcoli di dati derivati — tra cui il più semplice BMI e numerosi altri calcoli più complessi derivati dalla post-elaborazione dei dati inseriti — carte del rischio, indici vari, alert di diverso grado che implicano scelte mediche e calcolatori posologici. Il calcolo del dosaggio del Coumadin, ad esempio, rientra addirittura nella Classe 2B;

- hanno avviato la certificazione MDR CE 2A dopo maggio 2024, non erano certificati MDR CE I prima di tale data e si trovano ancora all'inizio o nel mezzo delle varie fasi certificative;
- hanno effettuato, dopo maggio 2024, una certificazione MDR CE I per funzioni che rientrano chiaramente nella Classe MDR CE 2X.

La domanda sul perché determinati software risultino presenti nel portale del Ministero della Salute, che può essere consultato per verificare quanto registrato, trova risposta nel fatto che la Classe CE I è basata su un'autodichiarazione.

In questi casi, alla non compliance possono aggiungersi ulteriori profili giuridici a carico della Software House che ha effettuato un'autocertificazione non conforme rispetto alla Classe di appartenenza.

Questo livello di approssimazione e di non compliance è stato possibile fino a oggi perché i controlli non erano ancora stati avviati in modo sistematico.

Ora il Ministero della Salute ha strutturato la direzione CE MDR nell'ambito dei software clinico-sanitari e i controlli sono già partiti nel settore dei software ospedalieri. A breve riguarderanno anche la Medicina Generale.

Cogliamo inoltre l'occasione per ringraziare i nostri clienti, che sostengono canoni certamente più elevati, perché tutte queste attività comportano costi molto significativi di sviluppo e di gestione del mantenimento della certificazione.

Questo consente di offrire prodotti più potenti, più tecnologici e, soprattutto, pienamente conformi alle normative.

Crediamo che i nostri clienti abbiano compreso bene le ragioni per cui a un prezzo molto basso può corrispondere un prodotto non professionale, ma soprattutto non conforme e potenzialmente fonte di numerosi problemi.

Naturalmente, i produttori che non sono compliant MDR CE 2 possono continuare a vendere e sviluppare i prodotti che da anni mettono a disposizione del mercato, ma, per non esporre i medici a rischi sanzionatori, devono rimuovere immediatamente tutte le funzionalità che rientrano nella Classe 2A.

Non è inoltre possibile inserire un semplice parametro che consenta di attivare o disattivare tali funzioni, poiché questa modalità è espressamente vietata dalla norma.

Millennium garantisce ai propri utenti di non trovarsi fuori norma e di non essere esposti a rischi di sanzioni.

Suggeriamo inoltre a tutti i medici che non utilizzano soluzioni Millennium di verificare con grande attenzione l'effettivo rispetto delle normative sopra citate da parte dei propri fornitori.

Si tratta ancora di una materia poco conosciuta, così come lo era inizialmente il tema del GDPR, che ha richiesto alcuni anni per entrare pienamente a regime.

Siamo ormai alla vigilia dell'avvio sistematico dei controlli e ne è prova anche la raccomandazione della FNOM-CEO di verificare che il proprio "gestionale" sia realmente compliant con tali norme.

Il vademecum è organizzato in tre livelli di approfondimento:

- una semplice elencazione delle norme;
- un sistema molto schematico di applicabilità e una sezione dedicata a domande e risposte;
- una parte più corposa di approfondimento.

Nella speranza di aver fatto cosa gradita e nel riconfermare che, da 42 anni, siamo sempre al fianco del Medico.

Vi auguriamo buona lettura.

Giorgio Moretti
Amministratore Delegato Millennium

Introduzione

Per un medico di medicina generale, oggi il software dello studio è molto più di uno strumento di lavoro: è un dispositivo medico. Questo contributo nasce per fare chiarezza su questo tema.

Spiegheremo perché il termine “gestionale di studio” è inadeguato: Lei sta usando un software clinico che deve rispettare tutte le norme sulla riduzione del rischio clinico previste dal Regolamento CE MDR, operativo dal 25 maggio 2024. In caso di inadempienza, il D.Lgs. 137 del 5 agosto 2022, che recepisce in Italia la normativa, prevede sanzioni da 20.000 a 120.000 euro per ogni medico.

Spiegheremo poi come le AFT debbano dotarsi di una soluzione di condivisione dei dati clinici che garantisca l'aggiornamento bidirezionale delle cartelle tra i medici della stessa AFT, anche se utilizzano software diversi; poiché sui dati di un paziente operano più soggetti, la consistenza in tempo reale è indispensabile per garantire il continuo allineamento delle cartelle cliniche. Non è possibile, ed è clinicamente rischioso, che il software di un medico non titolare che opera su un paziente non riaggiorni la cartella clinica del medico titolare: prescrizioni, nuovi problemi, vaccinazioni, ecc. Con le più recenti disposizioni GDPR, i rischi amministrativi e penali legati alla privacy sono sempre più critici.

Tratteremo le nuove disposizioni sui Data Center e gli obblighi per aziende come Millennium, che entro l'anno dovranno essere

certificate NIS2 secondo le norme ACN. L'obiettivo è ridurre il rischio di cybersecurity, sempre più esteso in sanità e con gravi conseguenze amministrative e contenziosi legali. Tutti i prodotti e i servizi offerti da un fornitore come Millennium operano solo in totale crittazione in Data Center compliant ACN.

Vi introdurremo anche alle norme in arrivo sull'uso dell'Intelligenza Artificiale che, in ambito sanitario, pongono limiti giustificati e interazioni complesse con MDR e GDPR, per cui questi strumenti vanno maneggiati con grande accortezza.

Infine, useremo questo piccolo contributo per richiamare i punti salienti della normativa sul Patient Summary, sulla nuova codifica ICD10-IM (al posto dell'ICD9-CM) e sul flusso SIAP, oltre a tutto ciò che deve ancora arrivare, anche se in forte ritardo, a beneficio della medicina generale con il Fascicolo Sanitario Elettronico 2.0.

Guida pratica per i medici di medicina generale

NORME, DISPOSIZIONI E SANZIONI

Il documento raccoglie, in forma operativa, gli adempimenti che incidono sull'attività quotidiana del medico: uso dei dispositivi e dei software clinici, tutela dei dati, sicurezza informatica e nuovi flussi informativi. Ogni sezione spiega che cosa controllare e quando chiedere supporto al fornitore o alla struttura sanitaria.

<i>Tema</i>	<i>Cosa deve fare l'MMG</i>	<i>Scadenza / stato</i>
MDR e software	Verificare marcatura, istruzioni e corretto utilizzo; segnalare gli incidenti.	MDR dal 26.05.2021; transizione fino al 2027/2028.
Classi di rischio	Rispettare istruzioni, tracciabilità e obblighi di vigilanza.	Classi I, IIa, IIb e III.
Vigilanza	Segnalare gli incidenti gravi al Ministero e al fabbricante.	Entro 10 giorni.
GDPR	Proteggere i dati, documentare i trattamenti e gestire i fornitori.	Applicabile dal 25.05.2018.

<i>Tema</i>	<i>Cosa deve fare l'MMG</i>	<i>Scadenza / stato</i>
NIS2	Applicare le misure di sicurezza previste, se si rientra nel perimetro.	Obblighi operativi dal 2026.
AI Act	Mantenere la decisione clinica e informare il paziente sull'uso dell'IA.	Regole generali dal 02.08.2026.
ISO 9001 e 27001	Standard volontari, utili ma non obbligatori per l'MMG.	Edizioni 2026 e 2022.
Patient Summary	Compilare, aggiornare e verificare i dati del paziente.	Obbligo operativo dal 30.09.2025.
SIAP	Registrare dati completi nella cartella clinica elettronica.	Mensile nel 2026; settimanale dal 2027.
ICD-10-IM	Prepararsi alla nuova codifica e alla relativa formazione.	Obbligatoria nei flussi NSIS dal 01.01.2027.
Millennium	Sistema di compliance strutturato; certificazione MDR e adeguamenti digitali in percorso avanzato.	Presidi attivi e miglioramento continuo.
Fonti	Consultare le fonti ufficiali e aggiornate.	Riferimenti vigenti.

INDICE

01 Orientamento	16
02 Dispositivi medici	21
03 Fabbrikante	28
04 Medico	32
05 Classi di rischio (I)	35
06 Classi di rischio (IIa-III)	37
07 Software medico	40
08 Incidenti	44
09 Dati sanitari	46
10 Cybersicurezza	50
11 Intelligenza artificiale	54
12 Standard	56
13 FSE 2.0	58
14 Flussi informativi	61
15 ICD-10	63
16 Sanzioni	64
17 Stato aziendale	67
17.1 Millennium: un sistema di compliance strutturato	67
17.2 Millennium: protezione dei dati, sicurezza e intelligenza artificiale	69
17.3 Millennium: servizi per la medicina generale	71
Fonti	73

Orientamento

COME ORIENTARSI TRA NORME E RESPONSABILITÀ

Prima delle singole norme serve una mappa. Non tutto ciò che viene chiamato “obbligo” pesa allo stesso modo, e non tutti i soggetti rispondono delle stesse cose.

Tre livelli da non confondere

<i>Livello</i>	<i>Esempi</i>	<i>Effetto pratico</i>
Norme cogenti	MDR, GDPR, NIS2, AI Act, decreti nazionali	Creano obblighi e, quando previsto, sanzioni
Obblighi organizzativi e contrattuali	ACN MMG, accordi regionali, capitolati, istruzioni del titolare	Vincolano il medico o il fornitore nel perimetro specifico
Standard volontari	ISO 9001, ISO/IEC 27001, ISO 13485	Strutturano controlli e possono essere certificati; non equivalgono alla conformità legale

Ruoli ricorrenti

- **Fabbricante MDR:** persona fisica o giuridica che fabbrica o rimette a nuovo un dispositivo, oppure lo fa progettare o fabbricare e lo commercializza con il proprio nome o marchio.
- **Medico utilizzatore:** usa il dispositivo secondo destinazione d'uso e istruzioni; concorre alla dispositivo-vigilanza. Non diventa fabbricante per il solo uso.
- **Titolare GDPR:** decide finalità e mezzi del trattamento. Il medico è spesso titolare per il proprio studio; il fornitore è di regola responsabile ex art. 28 per hosting e assistenza, salvo trattamenti propri.
- **Provider / deployer AI Act:** chi sviluppa o immette il sistema e chi lo usa sotto la propria autorità. Il medico utilizzatore professionale è normalmente deployer.
- **Soggetto NIS2:** soltanto l'entità che ricade nel perimetro e risulta identificata e registrata secondo il D.Lgs. 138/2024 e gli atti ACN.

Calendario

Il calendario che segue riepiloga, per ogni normativa, le principali date di entrata in vigore e le scadenze entro cui devono essere applicati i relativi obblighi.

Permette quindi di capire rapidamente:

- da quando una norma è applicabile;
- quali adempimenti riguardano i fabbricanti di dispositivi medici;
- quali scadenze interessano medici, strutture sanitarie e fornitori software;
- quali date costituiscono termini transitori e sono valide solo in presenza delle condizioni previste dalla normativa.

<i>Normativa</i>	<i>Date chiave</i>	<i>Obbligo per fabbricanti di DM e fornitori software</i>
GDPR	25.05.2018	Obbligatorio quando il fabbricante o il fornitore tratta dati come titolare o responsabile: protezione dei dati fin dalla progettazione, misure di sicurezza, accordi ex art. 28, gestione delle violazioni e diritti degli interessati.
NIS2 · D.Lgs. 138/2024	16.10.2024 15.01.2026 entro 10.2026	Obbligo diretto solo per i fabbricanti inclusi nel perimetro e identificati da ACN. Notifica degli incidenti significativi dal 15.01.2026 e misure di sicurezza di base entro ottobre 2026. Per gli altri restano rilevanti gli obblighi contrattuali e la sicurezza della filiera.

01 Orientamento

Normativa	Date chiave	Obbligo per fabbricanti di DM e fornitori software
MDR e vigilanza	25.05.2017 26.05.2021 26.05.2024 / 26.09.2024 18.03.2026 26.05.2026 31.12.2027 / 31.12.2028	Entrata in vigore nel 2017; MDR obbligatorio dal 26.05.2021 per i nuovi dispositivi. Per i dispositivi legacy: sistema di gestione qualità (QMS) e domanda all'organismo notificato entro il 26.05.2024, accordo scritto entro il 26.09.2024. Transizione fino al 2027 per classe III e IIb impiantabili e fino al 2028 per gli altri IIb, IIa e classe I interessati. Il 26.05.2026 riguarda gli impiantabili su misura di classe III. Il DM incidenti, in vigore dal 18.03.2026, disciplina le segnalazioni di operatori e pazienti; ai fabbricanti resta la vigilanza MDR. Le proroghe valgono solo se tutte le condizioni sono rispettate.
AI Act e L. 132/2025	02.02.2025 10.10.2025 02.08.2026 02.08.2028	Alfabetizzazione sull'IA e primi divieti dal 02.02.2025; legge italiana applicabile dal 10.10.2025; regole generali e trasparenza dal 02.08.2026. Per l'IA ad alto rischio incorporata in prodotti regolamentati, inclusi i dispositivi medici quando ricorrono le condizioni, obblighi del provider o fabbricante dal 02.08.2028.

01 Orientamento

Normativa	Date chiave	Obbligo per fabbricanti di DM e fornitori software
Patient Summary e FSE	01.09.2025 30.09.2025	Nessun obbligo legale diretto per il fabbricante di dispositivi medici. Il fornitore del software deve supportare tracciati e funzioni previsti se compresi nella destinazione d'uso o nel contratto. Compilazione e verifica restano in capo a MMG e PLS.
SIAP	01.01.2026 01.01.2027	Il decreto obbliga Regioni e Province autonome alla trasmissione: mensile nel 2026 e settimanale dal 2027. Per il fornitore del software l'adeguamento deriva dalle specifiche regionali, dal contratto e dalle funzioni dichiarate, non da un obbligo diretto come fabbricante MDR.
ICD-10-IM e CIPI	01.01.2027	Obbligatorie per i flussi NSIS interessati. Il fornitore di software clinico deve aggiornare classificazioni e mappature quando tali funzioni rientrano nel prodotto o nel contratto; non è un obbligo generale di certificazione MDR.
ISO 9001, ISO/IEC 27001, ISO 13485	Edizioni vigenti: 2026 / 2022 / 2016	Standard volontari, senza una data generale di obbligatorietà per i fabbricanti. Possono diventare vincolanti per contratto, gara o certificazione. L'MDR richiede un sistema qualità adeguato, ma non impone in via generale il certificato ISO 13485.

Dispositivi medici

MDR E DISPOSITIVI MEDICI

Regolamento (UE) 2017/745 e D.Lgs. 5 agosto 2022, n. 137

Date e principio guida

- Il Regolamento europeo sui dispositivi medici (**MDR**) è entrato in vigore il **25 maggio 2017** ed è diventato pienamente applicabile dal **26 maggio 2021**.
- In Italia, il Parlamento ha recepito il Regolamento europeo con il D.Lgs. 137 del 5 agosto 2022, che ha definito le autorità competenti, le attività di vigilanza e le sanzioni applicabili in caso di violazione della normativa.
- Dal 26 maggio 2021, ogni nuovo dispositivo medico immesso sul mercato deve rispettare i requisiti previsti dall'MDR. Le proroghe fino al 2027 o al 2028 non si applicano automaticamente a tutti i dispositivi: riguardano esclusivamente alcuni prodotti già certificati secondo la precedente normativa, denominati "legacy devices", e solo quando il fabbricante rispetta tutte le condizioni previste dal Regolamento (UE) 2023/607.

Il periodo transitorio

Dal 25 maggio 2024 è pienamente in vigore la normativa CE MDR, con un periodo transitorio strettamente regolamentato: i prodotti già esistenti a quella data e già certificati MDD CE o MDR CE classe I restano in regola solo se sono stati compiuti i passaggi formali per portarli alla certificazione MDR CE entro il 31 dicembre 2028. Tutti i prodotti che non hanno seguito questo iter sono fuori norma. Da tale data, ogni nuovo dispositivo medico immesso sul mercato deve rispettare i requisiti dell'MDR; le proroghe fino al 2027 o al 2028 restano riservate ai soli "legacy devices" che soddisfano tutte le condizioni del Regolamento (UE) 2023/607.

I controlli sono partiti

Nella primavera 2025 il Ministero della Salute ha costituito al proprio interno una sezione dedicata alla vigilanza sull'applicazione dell'art. 11 del Regolamento europeo, composta da personale dedicato alla valutazione dei prodotti e al monitoraggio del mercato. Nell'estate 2025 sono partite le attività ispettive, concentrate in primo luogo sui prodotti software ospedalieri e destinate, a breve, a estendersi ai prodotti della Medicina Generale.

Elementi sostanziali derivati dal Regolamento europeo (art. 11)

- Un software è considerato dispositivo medico quando il fabbricante dichiara che è destinato, ad esempio, a supportare una diagnosi, una decisione terapeutica, il monitoraggio di una patologia o la previsione di un rischio clinico riferito al singolo paziente.
- Non sono invece automaticamente dispositivi medici i programmi utilizzati soltanto per archiviare documenti, gestire appuntamenti e fatture, comunicare informazioni o effettuare semplici ricerche.

IN PRATICA, PER L'MMG

Prima di utilizzare una funzione software a supporto dell'attività clinica è opportuno verificare la destinazione d'uso dichiarata dal produttore, la presenza della marcatura CE e le istruzioni per l'uso. Non è sufficiente che un programma venga utilizzato in ambito sanitario perché sia automaticamente qualificato come dispositivo medico.

Chi risponde di cosa

La responsabilità dell'utilizzo del prodotto software che dispone di funzionalità ricadenti nelle classi CE MDR è del medico, che deve verificare se tali funzionalità sono compliant con la corretta marcatura CE MDR.

Il medico che utilizza prodotti non certificati che contengono funzionalità soggette alla specifica certificazione CE MDR viene sanzionato sulla base dell'art. 27 del D.Lgs. 137/2022, con una sanzione tra 24.200 e 145.000 euro.

Il fabbricante — come lo definisce il Regolamento europeo, ossia la software house — che immette sul mercato prodotti per i quali esiste l'obbligo di certificazione CE MDR **viene sanzionato sulla base dell'art. 27 del D.Lgs. 137/2022, con una sanzione tra 24.200 e 145.000 euro.**

La software house che dichiara di disporre di funzionalità certificate CE MDR in una classe non coerente viene sanzionata sulla base dell'art. 27, con una sanzione tra 24.200 e 145.000 euro, oltre a essere oggetto di potenziale rivalsa sul piano civile e penale per false dichiarazioni.

Questo non libera comunque il medico dalla responsabilità di verificare la corretta marcatura CE, né lo esenta dalle sanzioni.

Come capire se un software è un dispositivo medico e ricade nell'MDR

Ha una finalità medica?

Il software può essere un dispositivo medico se viene utilizzato per diagnosticare una malattia, prevederne l'evoluzione, monitorare il paziente, suggerire un trattamento o supportare una decisione clinica riferita al singolo assistito.

Elabora i dati del paziente?

È rilevante quando il software analizza i dati e produce una nuova informazione clinica, ad esempio un punteggio di rischio, un allarme, un'ipotesi diagnostica o una proposta terapeutica. La semplice archiviazione, visualizzazione o trasmissione dei dati, di norma, non è sufficiente.

Qual è la destinazione d'uso dichiarata?

Conta l'uso indicato dal fabbricante nelle istruzioni, nella documentazione e nel materiale informativo. Non è il nome del prodotto o l'uso deciso autonomamente dal medico a stabilire se si tratta di un dispositivo medico.

Il prodotto contiene più funzioni o moduli?

Un programma può includere sia funzioni amministrative sia funzioni cliniche. La qualificazione come dispositivo medico può quindi riguardare soltanto uno specifico modulo, ad esempio quello che elabora i dati e fornisce un supporto decisionale.

IN PRATICA, PER L'MMG

Un normale gestionale utilizzato per registrare dati, prescrizioni o appuntamenti non è necessariamente un dispositivo medico. Può invece esserlo la funzione che analizza le informazioni del paziente e genera avvisi, valutazioni del rischio o indicazioni utili alla decisione clinica. La qualificazione è responsabilità del fabbricante e deve risultare chiaramente dalla documentazione del prodotto.

Regime transitorio: controllo documentale

Alcuni dispositivi già immessi sul mercato con una certificazione valida secondo le precedenti direttive europee possono continuare a essere forniti e utilizzati anche dopo l'entrata in applicazione dell'MDR.

Questo non significa che siano privi di certificazione o non conformi: la normativa europea consente temporaneamente il mantenimento della precedente marcatura CE, purché il fabbricante abbia avviato nei termini il percorso di adeguamento all'MDR e rispetti tutte le condizioni previste.

- fino al **31 dicembre 2027**, per i dispositivi di classe III e per alcuni dispositivi impiantabili di classe IIb;
- fino al **31 dicembre 2028**, per gli altri dispositivi di classe IIb, per quelli di classe IIa e per alcuni dispositivi precedentemente classificati in classe I che, con l'MDR, richiedono l'intervento di un organismo notificato.

Queste scadenze non costituiscono una proroga automatica della precedente certificazione. Il fabbricante può beneficiare del periodo transitorio solo se ha rispettato tutte le condizioni previste: il dispositivo non deve presentare rischi inaccettabili, non deve aver subito modifiche significative nella progettazione

02 Dispositivi medici

o nella destinazione d'uso e deve essere stato avviato nei termini il percorso di adeguamento all'MDR, compresa la richiesta e il successivo accordo con un organismo notificato.

IN PRATICA, PER L'MMG

La presenza, su un dispositivo o su un software, di una certificazione rilasciata secondo la precedente normativa non significa necessariamente che il prodotto sia irregolare.

Può trattarsi di un dispositivo legittimamente commercializzato nel periodo transitorio. In caso di dubbio, il medico può chiedere al fornitore la dichiarazione di conformità, il certificato precedente e, quando applicabile, la documentazione che conferma l'avvio del percorso MDR con l'organismo notificato.

Non spetta all'MMG verificare direttamente tutte le condizioni amministrative del fabbricante, ma è opportuno utilizzare il prodotto secondo la destinazione d'uso e le istruzioni fornite.

Fabbricante

COSA DEVE GARANTIRE IL FABBRICANTE

In questo capitolo il focus è sul fabbricante, a cui spetta il grosso degli adempimenti. Per il medico di medicina generale il compito è più semplice e operativo: non serve spulciare l'intero fascicolo tecnico, ma occorre saper riconoscere un prodotto a norma, usarlo seguendo le istruzioni e segnalare tempestivamente eventuali anomalie.

Fase	Cosa deve fare il fabbricante	Cosa interessa all'MMG
Qualificazione e classe di rischio	Stabilire se il prodotto è un dispositivo medico, definirne con precisione la finalità e attribuirgli la corretta classe di rischio. Per i software è particolarmente importante la Regola 11 dell'Allegato VIII MDR.	La destinazione d'uso e le funzioni cliniche devono essere descritte chiaramente e in modo coerente nelle istruzioni, sul sito e nel materiale informativo
Sistema di gestione per la qualità	Organizzare e controllare progettazione, sviluppo, fornitori, reclami, modifiche e attività successive alla commercializzazione. La ISO 13485 è lo standard normalmente utilizzato, ma non sostituisce gli obblighi dell'MDR.	Il medico deve poter ricevere assistenza, aggiornamenti, informazioni di sicurezza e risposte alle segnalazioni relative al prodotto.

03 Fabbricante

Fase	Cosa deve fare il fabbricante	Cosa interessa all'MMG
Gestione dei rischi	Individuare i possibili pericoli, adottare misure di prevenzione e verificare che i rischi residui siano accettabili. Per un software devono essere considerati anche errori di utilizzo, indisponibilità del sistema e rischi informatici.	L'MMG deve conoscere le avvertenze e i limiti del prodotto, evitando di utilizzare le indicazioni del software come sostituzione automatica della propria valutazione clinica.
Valutazione clinica	Dimostrare, mediante dati adeguati, che il dispositivo è sicuro, offre le prestazioni dichiarate e produce il beneficio clinico previsto.	Le prestazioni pubblicizzate devono corrispondere alla destinazione d'uso e alle indicazioni riportate nella documentazione ufficiale.
Sviluppo e verifica	Documentare come il prodotto è stato progettato e testato, verificando che funzioni correttamente, sia sicuro e risponda ai requisiti previsti. Ogni aggiornamento deve essere controllato e tracciato.	Gli aggiornamenti devono provenire da canali autorizzati. Il medico deve evitare versioni non supportate o modifiche non approvate dal fabbricante.

03 Fabbricante

Fase	Cosa deve fare il fabbricante	Cosa interessa all'MMG
Valutazione della conformità	Seguire la procedura prevista dall'articolo 52 MDR. Per le classi IIa, IIb e III è necessario l'intervento di un organismo notificato; per alcuni dispositivi di classe I il suo intervento è limitato a specifici aspetti.	Il prodotto deve essere accompagnato dalla marcatura CE e dalla dichiarazione UE di conformità. Quando previsto, accanto alla marcatura CE compare il numero dell'organismo notificato.
Registrazione e UDI	Registrare il fabbricante e il dispositivo nelle banche dati previste e attribuire il codice UDI, che consente l'identificazione e la tracciabilità del prodotto.	L'UDI e i dati identificativi aiutano a riconoscere esattamente dispositivo, versione e fabbricante, soprattutto in caso di segnalazioni o richiami.
Sorveglianza e vigilanza	Controllare il comportamento del dispositivo dopo la commercializzazione, raccogliere reclami, analizzare gli incidenti e adottare eventuali azioni correttive o richiami di sicurezza.	L'MMG deve comunicare tempestivamente malfunzionamenti, incidenti o situazioni potenzialmente pericolose, indicando quando possibile prodotto, versione e circostanze dell'evento.
PRRC	Nominare una persona responsabile del rispetto della normativa, dotata delle competenze necessarie e incaricata di controllare la conformità del dispositivo.	Per l'MMG è una garanzia organizzativa: significa che il fabbricante ha individuato formalmente una figura responsabile della conformità regolatoria.

IN SINTESI

L'MMG non deve “certificare” il dispositivo né controllare tutta la documentazione del fabbricante. Prima dell'utilizzo deve però verificare che il prodotto sia chiaramente identificato, destinato all'uso clinico previsto e accompagnato dalle informazioni necessarie. Durante l'impiego deve rispettare le istruzioni e segnalare eventuali incidenti o malfunzionamenti.

Obbligo continuo, non “certificato una volta”

Il marchio CE attesta il completamento della procedura pertinente alla versione e alla destinazione d'uso. Ogni modifica, vulnerabilità, segnale clinico o reclamo deve essere valutato per il suo impatto su rischi, documentazione, certificato e comunicazioni.

Medico

COSA DEVE FARE IL MEDICO PRIMA, DURANTE E DOPO L'USO

Consigli operativi per usare software e dispositivi clinici con la giusta consapevolezza

Prima di utilizzare il dispositivo o il software

Prima di adottare uno strumento, il medico dovrebbe verificare che la funzione proposta sia effettivamente prevista dal fabbricante e che il prodotto sia regolarmente disponibile sul mercato. Le informazioni essenziali sono la marcatura CE, la destinazione d'uso e la versione del prodotto.

È importante conoscere le istruzioni, le controindicazioni e i limiti del sistema. Una breve formazione iniziale, soprattutto per i software di supporto decisionale, riduce il rischio di interpretare il risultato fuori dal contesto per cui è stato validato.

Il medico deve inoltre sapere chi è il fabbricante e come contattarlo per assistenza, reclami o segnalazioni. Anche gli aggiornamenti di sicurezza devono provenire da canali riconoscibili e affidabili.

Le formule commerciali sintetiche non sostituiscono la documentazione del prodotto. Quando necessario, è corretto chiedere al fornitore un riferimento preciso al prodotto, alla versione e al relativo stato regolatorio.

Durante l'attività clinica

Il risultato di un sistema di supporto decisionale è un aiuto alla valutazione. La decisione resta del medico e deve essere confrontata con anamnesi, esame obiettivo, terapie, linee guida e situazione concreta del paziente.

Il dispositivo deve essere utilizzato nei limiti indicati dal fabbricante, con le configurazioni previste e con gli aggiornamenti di sicurezza disponibili.

Quando l'output del software incide sul percorso di cura, è opportuno registrare in cartella gli elementi clinici che hanno portato alla decisione finale, senza limitarsi a copiare automaticamente il suggerimento.

Credenziali personali, blocco dello schermo, aggiornamenti e segnalazione tempestiva delle anomalie sono parte dell'uso corretto del sistema, al pari delle normali precauzioni cliniche.

Se il risultato appare errato o il sistema non funziona

<i>Evento</i>	<i>Azione</i>
Incidente grave, anche solo sospetto	Mettere in sicurezza il paziente e conservare le evidenze; segnalare al Ministero entro 10 giorni; informare il fabbricante secondo il D.Lgs. 137/2022 e la procedura locale.
Incidente non grave	Può essere segnalato al Ministero entro 30 giorni; comunicare al fabbricante e seguire la procedura regionale o della struttura.
Reclamo o malfunzionamento senza incidente	Registrare dettagli, versione e log; comunicare al fabbricante e seguirne gli esiti.
Avviso di sicurezza / FSCA	Leggere e attuare tempestivamente: aggiornamento, quarantena, richiamo, modifica del flusso o comunicazione ai pazienti.

SANZIONE SPECIFICA

L'omessa comunicazione dell'incidente grave prevista dall'art. 10, c. 2, D.Lgs. 137/2022 espone l'operatore sanitario o il referente alla sanzione amministrativa da 26.000 a 120.000 euro (art. 27, c. 45).

Classi di rischio (I)

CLASSE I E DISPOSITIVI A RISCHIO PIÙ BASSO

La classificazione spetta sempre al fabbricante: gli esempi riportati hanno valore puramente indicativo e variano in base alla specifica destinazione d'uso.

Classe	Tipologie / esempi indicativi	Obblighi del fabbricante	Cosa significa per l'MMG
I	Dispositivi non invasivi o a basso rischio: ausili semplici, stetoscopi meccanici, occhiali; software che non ricade nelle fattispecie più rischiose della Regola 11. La classe non si deduce dal nome.	Autocertificazione possibile; sistema di gestione qualità (QMS) MDR, fascicolo tecnico, valutazione clinica, rischi, rapporto PMS, UDI/registrazione e dichiarazione UE. Nessun organismo notificato per la conformità ordinaria.	Controllare marcatura e istruzioni, usare il dispositivo come previsto e segnalare problemi o incidenti. Verificare che le funzioni del software non contengano sistemi di calcolo di metadati clinici, gestione delle interazioni tra farmaci, calcolatori posologici, alert di ogni tipologia, scale del rischio, sistemi di supporto alla decisione basati su IA non certificate: se presenti, la classe I non è più coerente.
Is	Classe I fornito sterile: alcuni dispositivi non invasivi sterili.	Come classe I, ma con organismo notificato limitatamente agli aspetti di sterilità.	Controllare confezione, scadenza e conservazione. Non utilizzare il prodotto se la sterilità può essere compromessa.

05 Classi di rischio (I)

Classe	Tipologie / esempi indicativi	Obblighi del fabbricante	Cosa significa per l'MMG
Im	Classe I con funzione di misura: alcuni misuratori semplici, se classificati I dalla regola applicabile.	Organismo notificato limitatamente agli aspetti metrologici; controlli di calibrazione e prestazione.	Rispettare controlli e manutenzione e non affidarsi a misure che risultano incoerenti.
Ir	Strumenti chirurgici riutilizzabili di classe I.	Organismo notificato limitatamente al riutilizzo: pulizia, disinfezione, sterilizzazione, manutenzione e test funzionali.	Seguire le istruzioni per pulizia, sterilizzazione e riutilizzo, conservandone la tracciabilità.

Nota sulla classe I “legacy”

Un dispositivo già classe I secondo la precedente direttiva (MDD) che resta classe I con l'MDR non ottiene automaticamente la proroga al 2028: la transizione riguarda, tra gli altri, gli ex classe I che sotto MDR necessitano per la prima volta dell'intervento di un organismo notificato. Va verificata la fattispecie concreta.

UDI e studio medico

L'obbligo italiano di registrare e conservare l'UDI da parte di istituzioni e professionisti sanitari dipende dai decreti attuativi e considera la classe di rischio. L'MDR impone almeno la conservazione dell'UDI dei dispositivi impiantabili di classe III alle istituzioni sanitarie; per lo studio dell'MMG va applicata la disciplina nazionale e regionale pertinente, senza generalizzare a ogni software.

Classi IIa, IIb e III: cosa cambia

DALLA CLASSE IIA ALLA III, IL RUOLO DELL'ORGANISMO
NOTIFICATO DIVENTA VIA VIA PIÙ CENTRALE E STRINGENTE

<i>Classe</i>	<i>Tipologie / esempi indicativi</i>	<i>Obblighi del fabbricante</i>	<i>Cosa significa per l'MMG</i>
IIa	Dispositivi invasivi a breve termine e molti dispositivi attivi diagnostici o terapeutici; software che fornisce informazioni per decisioni diagnostiche o terapeutiche quando le conseguenze non raggiungono le soglie IIb/III; software che monitora processi fisiologici non vitali.	Organismo notificato per il sistema qualità e la documentazione secondo l'art. 52; valutazione clinica e PMCF; PMS; PSUR almeno ogni 2 anni; UDI/registrazione; vigilanza.	Conoscere versione e limiti del dispositivo, mantenere la supervisione clinica e segnalare risultati anomali o incidenti. Rientrano in questa classe le funzioni software con calcolo di metadati clinici, gestione delle interazioni tra farmaci, calcolatori posologici non salvavita, alert che non ricadono nella definizione di allarmi salvavita, scale del rischio, sistemi di supporto alla decisione basati su IA non certificate.

06 Classi di rischio (IIa-III)

Classe	Tipologie / esempi indicativi	Obblighi del fabbricante	Cosa significa per l'MMG
IIb	Rischio medio-alto: ventilatori, molte pompe di infusione, dispositivi invasivi a lungo termine; software le cui decisioni possono causare grave deterioramento o intervento chirurgico, o monitoraggio di parametri vitali con pericolo immediato.	Organismo notificato con valutazione più intensa; evidenza clinica robusta; PMCF; PSUR almeno annuale; controlli di progettazione e cybersecurity; sorveglianza post-market.	Verificare versione e aggiornamenti, controllare autonomamente i risultati più delicati e applicare subito gli avvisi di sicurezza. Rientrano in questa classe le funzioni software con calcolo di metadati clinici, gestione delle interazioni tra farmaci, calcolatori posologici su farmaci salvavita o a rischio clinico alto fino alla morte (ad esempio il dosaggio del Coumadin), alert che ricadono nella definizione di allarmi salvavita, scale del rischio, sistemi di supporto alla decisione basati su IA non certificate.
III	Rischio alto: pacemaker, valvole cardiache, impianti mammari; software quando le decisioni possono provocare morte o deterioramento irreversibile.	Organismo notificato; massima robustezza clinica e regolatoria; possibili procedure di consultazione; PSUR annuale; SSCP per le classi pertinenti; carta impianto per gli impiantabili; PMS/ PMCF intensivi.	Non basare la decisione sul solo output. Garantire tracciabilità, follow-up e segnalazione tempestiva di ogni problema.

Regola 11 del software: schema pratico

<i>Funzione del software</i>	<i>Classe di base</i>
Informazione usata per decisioni diagnostiche o terapeutiche	IIa; IIb se possibile grave deterioramento o intervento; III se possibile morte o deterioramento irreversibile
Monitoraggio di processi fisiologici	IIa; IIb se parametri vitali e variazioni possono creare pericolo immediato.
Altro software	I, fermo il controllo delle altre regole e della destinazione d'uso.

Fonte interpretativa: MDCG 2019-11 rev.1 (giugno 2025). La classificazione finale richiede l'analisi della destinazione d'uso, dell'azione sull'informazione e delle conseguenze cliniche.

Software medico

SOFTWARE MEDICO E AGGIORNAMENTI: COSA CONTROLLARE

Aggiornamenti software: quando e come cambia l'inquadramento regolatorio.

Quattro controlli per ogni release

Controllo	Domande da porsi	In parole semplici
Perimetro	Quale modulo o versione è il dispositivo? Le funzionalità non mediche sono separate e chiaramente descritte?	Capire che cosa è regolato: non tutto il programma lo è, ma il confine deve essere chiaro.
Destinazione d'uso	Sono cambiati popolazione, patologia, utenti, ambiente, output o ruolo nella decisione?	Verificare che il software faccia ancora ciò per cui è stato dichiarato, per gli stessi pazienti e utenti.
Rischio e clinica	Nuovi dati, regole, modelli IA, interfacce o fonti informative introducono pericoli o cambiano prestazioni e beneficio?	Accertare che le novità non aggiungano rischi né alterino l'affidabilità dei risultati.
Significatività	Per un legacy device, la modifica è "significativa" rispetto a design o destinazione d'uso? Se sì, la transizione può cessare.	Per i prodotti ancora in regime transitorio, una modifica rilevante può far perdere la proroga.

Interoperabilità non significa trasferire la responsabilità

<i>Chi</i>	<i>Che cosa deve garantire</i>
Il fabbricante	Definire interfacce, formati, requisiti minimi, gestione degli errori, sicurezza e configurazioni validate.
Il medico	Verificare l'avvenuta acquisizione dei dati rilevanti, soprattutto dopo migrazioni, integrazioni con FSE e SIAP o aggiornamenti.
Il titolare privacy	Sapere dove transitano e risiedono i dati, chi vi accede, quali sub-responsabili operano e come si gestiscono indisponibilità e perdita dei dati.
Componenti IA o di terzi	La catena contrattuale deve assicurare documentazione, log, monitoraggio, gestione degli incidenti e controllo delle modifiche.

Segnali di attenzione nella documentazione

Prima di utilizzare un dispositivo o un software clinico, l'MMG dovrebbe prestare attenzione ad alcuni elementi che possono indicare una documentazione incompleta o poco chiara. Sono cinque:

1. **Marcatura CE non verificabile.** Il simbolo CE compare sul prodotto o sul sito, ma non è disponibile la dichiarazione UE di conformità, oppure il documento non permette di identificare con chiarezza il nome e la versione del dispositivo.
2. **Certificato non adeguato.** Il certificato dell'organismo notificato è scaduto, riguarda un prodotto diverso oppure attesta solamente il sistema qualità del fabbricante. Una certificazione ISO del sistema qualità, da sola, non dimostra la conformità MDR del dispositivo.
3. **Funzioni cliniche non coerenti con la destinazione d'uso.** Il software viene pubblicizzato come strumento capace di formulare diagnosi, calcolare rischi o suggerire terapie, mentre nella documentazione ufficiale è descritto soltanto come programma gestionale. Le funzioni dichiarate nel materiale commerciale devono essere coerenti con quelle autorizzate dal fabbricante.
4. **Dichiarazioni generiche di conformità.** Espressioni come “certificato MDR”, “GDPR compliant” o “NIS2 compliant” devono essere accompagnate da informazioni che chiariscano a quale prodotto, versione, attività o certificato si riferiscono. GDPR e NIS2, in particolare, non prevedono una generica marcatura del prodotto equivalente alla marcatura CE.
5. **Aggiornamenti non documentati.** Un aggiornamento obbligatorio dovrebbe indicare almeno la nuova versione, le modifiche introdotte e gli eventuali effetti sulla sicurezza o sull'utilizzo. Dopo l'installazione deve essere possibile verificare quale versione del software è attiva.

Risultato anomalo: cosa fare

Se il software restituisce un risultato incoerente con i dati clinici, genera un allarme errato o presenta un malfunzionamento potenzialmente pericoloso, l'MMG **non deve basare la propria decisione esclusivamente su quell'indicazione**. È opportuno:

1. **verificare** la situazione clinica con strumenti o fonti alternative;
2. **interrompere**, se possibile, l'utilizzo della funzione interessata;
3. **annotare** il nome del prodotto, la versione, la data e le circostanze dell'anomalia;
4. **conservare** eventuali schermate o messaggi di errore, evitando diffusioni non autorizzate dei dati del paziente;
5. **contattare** l'assistenza e informare il fabbricante;
6. **attivare**, quando ricorrono le condizioni, la procedura di segnalazione dell'incidente.

LA PRIORITÀ

Resta sempre la tutela del paziente: il software supporta l'attività del medico, ma non sostituisce la valutazione clinica dell'MMG.

Incidenti

GESTIONE INCIDENTI: LA CHECKLIST PER L'MMG

DM 1° luglio 2025, in vigore dal 18 marzo 2026.

Flusso operativo dell'MMG

Passo	Cosa fare
1. Assistenza	Proteggere il paziente; non ritardare le cure urgenti. Se utile, mettere in sicurezza il dispositivo senza alterare le evidenze.
2. Evidenze	Annotare data e ora, dispositivo, UDI se disponibile, versione software, output, contesto, conseguenze e log; evitare dati identificativi nel modulo nazionale.
3. Ministero	Incidente grave, anche solo sospetto: modulo online, tempestivamente e comunque entro 10 giorni dalla conoscenza. Incidente non grave: facoltà di segnalare entro 30 giorni.
4. Fabbricante	Comunicare incidenti e reclami secondo l'art. 10 del D.Lgs. 137/2022 e i canali indicati; conservare ricevuta e follow-up.
5. Azioni	Applicare avvisi di sicurezza (FSCA), aggiornamenti o quarantena; identificare i pazienti interessati se necessario.

Sanzioni chiave (D.Lgs. 137/2022)

Soggetto / violazione	Sanzione amministrativa
Operatore sanitario o referente: omessa comunicazione di incidente grave ex art. 10, c. 2	€26.000–€120.000 (art. 27, c. 45)
Fabbricante: omessa vigilanza, segnalazione, indagine o azioni ex artt. 87-89 MDR	€24.200–€145.000 (art. 27, c. 44)
Immissione o messa in servizio in violazione dell'art. 5 MDR	€24.200–€145.000 (art. 27, c. 1)
Mancata procedura di valutazione della conformità ex art. 52	€26.000–€120.000 (art. 27, c. 32)
Claim ingannevoli vietati dall'art. 7 MDR	€2.800–€11.300 (fattispecie prevista dall'art. 27)

Gli importi possono essere aggiornati e si applicano secondo fattispecie, responsabilità, cumulo e criteri della L. 689/1981. Restano possibili responsabilità civile, penale, disciplinare e deontologica.

Dati sanitari

DATI DEI PAZIENTI: LE REGOLE ESSENZIALI PER L'MMG

L'MMG tratta quotidianamente dati particolarmente delicati, come diagnosi, terapie, prescrizioni e referti. Per i trattamenti svolti nel proprio studio, il medico opera normalmente come titolare del trattamento ed è quindi responsabile delle modalità con cui i dati vengono raccolti, utilizzati, conservati e protetti.

Obblighi principali dell'MMG

Area	Cosa deve fare concretamente l'MMG
Base giuridica	Per utilizzare i dati necessari alla diagnosi, alla cura e alla prevenzione non è normalmente richiesto il consenso privacy del paziente. Il trattamento è consentito perché necessario per finalità sanitarie. Il consenso può invece essere necessario per finalità ulteriori, come marketing, comunicazioni non connesse alla cura o alcune attività di ricerca.
Informativa	Il paziente deve ricevere un'informativa chiara che spieghi quali dati vengono trattati, per quali finalità, per quanto tempo, con chi possono essere condivisi e come esercitare i propri diritti. L'informativa non coincide con una richiesta di consenso.
Organizzazione dello studio	Il medico deve tenere aggiornato il registro dei trattamenti, stabilire tempi di conservazione, autorizzare formalmente collaboratori e sostituti e fornire loro adeguate istruzioni. Chi accede ai dati deve farlo solo per le attività assegnate.

Obblighi principali dell'MMG

Area	<i>Cosa deve fare concretamente l'MMG</i>
Fornitori informatici	Se il gestionale, il cloud o l'assistenza tecnica possono accedere ai dati dei pazienti, il fornitore deve essere nominato responsabile del trattamento mediante un contratto conforme all'art. 28 GDPR. Il contratto deve disciplinare sicurezza, riservatezza, subfornitori, incidenti e restituzione o cancellazione dei dati.
Sicurezza degli accessi	Ogni operatore deve utilizzare un proprio account. Le password non devono essere condivise e, quando disponibile, deve essere attivata l'autenticazione a più fattori. Sono inoltre necessari aggiornamenti, antivirus, backup verificati, protezione dei dispositivi e blocco dello schermo.
Valutazione dei rischi	Quando un trattamento può comportare rischi elevati per i pazienti, ad esempio per l'impiego di nuove tecnologie o l'elaborazione sistematica di molti dati sanitari, può essere necessaria una DPIA, cioè una valutazione preventiva dell'impatto sulla protezione dei dati.
Violazione dei dati	Smarrimento di dispositivi, accessi abusivi, invio di documenti al destinatario sbagliato, attacchi informatici o indisponibilità dei dati devono essere comunicati immediatamente al referente privacy. Se previsto, la violazione deve essere notificata al Garante entro 72 ore dalla conoscenza dell'evento.

Obblighi del fornitore del software

Il fornitore deve progettare e gestire il servizio adottando misure adeguate alla delicatezza dei dati sanitari. In particolare, deve:

- proteggere i dati fin dalla progettazione del prodotto;
- registrare e limitare gli accessi;
- gestire aggiornamenti, vulnerabilità e incidenti;
- assistere il medico in caso di data breach o richiesta del paziente;
- restituire o cancellare i dati alla cessazione del servizio;
- non utilizzare i dati dei pazienti per finalità proprie non autorizzate.

La dichiarazione **“GDPR compliant”** non è sufficiente da sola: il fornitore dovrebbe essere in grado di indicare concretamente le misure adottate, la localizzazione dei dati e gli eventuali subfornitori coinvolti.

Fascicolo Sanitario Elettronico

L'alimentazione del FSE e la sua consultazione sono attività distinte. Il medico deve formare e trasmettere i documenti previsti secondo le regole nazionali e regionali; il paziente conserva il controllo sulla consultazione del fascicolo e può revocare il relativo consenso. Può inoltre chiedere l'oscuramento di determinati dati o documenti, che non saranno visibili agli altri professionisti autorizzati.

Sanzioni

Il GDPR prevede sanzioni fino a **10 milioni di euro o al 2% del fatturato mondiale** per alcune violazioni organizzative e di sicurezza e fino a **20 milioni di euro o al 4% del fatturato** per le violazioni più gravi.

Questi sono limiti massimi: l'importo effettivo viene stabilito considerando gravità, durata, numero di persone coinvolte, misure di sicurezza adottate e collaborazione con l'Autorità.

IN PRATICA, PER L'MMG

L'MMG non deve chiedere al paziente di firmare un generico “consenso privacy” per poterlo curare. Deve invece informarlo correttamente, proteggere i dati, scegliere fornitori affidabili e sapere come intervenire in caso di errore, perdita o accesso non autorizzato.

Cybersicurezza

SICUREZZA INFORMATICA E NIS2

La NIS2 impone alle organizzazioni che rientrano nel suo campo di applicazione di proteggere reti, sistemi e servizi digitali e di gestire correttamente gli incidenti informatici.

Il fabbricante deve essere certificato?

La NIS2 **non prevede il rilascio di un certificato o di un marchio “NIS2”**. Il fabbricante, quando rientra tra i soggetti individuati dalla normativa e da ACN, deve dimostrare di avere concretamente adottato le misure richieste.

I fabbricanti di dispositivi medici e di dispositivi diagnostici in vitro sono compresi tra i settori considerati dalla normativa. L'applicazione dipende però dalle dimensioni dell'impresa, dalla tipologia di attività, dall'eventuale produzione di dispositivi considerati critici e dall'inserimento nell'elenco dei soggetti NIS tenuto da ACN.

La certificazione **ISO/IEC 27001** non è generalmente obbligatoria, ma rappresenta una buona evidenza dell'esistenza di un sistema organizzato per la sicurezza delle informazioni. Non sostituisce comunque gli adempimenti previsti dalla NIS2. ACN ha infatti previsto specifici strumenti per aiutare le organizzazioni già certificate ISO 27001 ad allinearsi ai requisiti NIS2.

Obblighi e buone pratiche del fabbricante

<i>Situazione</i>	<i>Cosa deve fare il fabbricante</i>
Fabbricante inserito nel perimetro NIS2	Deve registrarsi secondo le modalità ACN, adottare le misure di sicurezza previste, formare direzione e personale, controllare i fornitori, predisporre continuità operativa e notificare gli incidenti significativi.
Fabbricante non soggetto direttamente alla NIS2	Deve comunque garantire un livello di sicurezza adeguato in base al GDPR, all'MDR e agli impegni contrattuali. Per un dispositivo medico software la cybersecurity deve essere gestita durante tutto il ciclo di vita del prodotto.
Fabbricante certificato ISO/IEC 27001	Deve indicare chiaramente quale società, sede, prodotto o servizio rientra nel certificato. La sola presenza del logo ISO 27001 non dimostra che ogni prodotto aziendale sia coperto dalla certificazione.
Fornitore software o cloud	Deve garantire protezione degli accessi, aggiornamenti di sicurezza, gestione delle vulnerabilità, backup, ripristino dei servizi e comunicazione tempestiva degli incidenti.
Gestione degli incidenti	Se soggetto NIS2, deve effettuare una pre-notifica entro 24 ore, una notifica entro 72 ore e una relazione finale, di norma entro un mese, quando l'incidente presenta i requisiti di significatività previsti.

Cosa deve controllare l'MMG

L'MMG non è tenuto a svolgere un audit informatico sul fabbricante e non deve verificare personalmente tutta la conformità NIS2. Prima di utilizzare un software che tratta dati sanitari o supporta decisioni cliniche, è però opportuno verificare che il fornitore dia risposte chiare almeno sui seguenti aspetti:

- presenza di un referente per sicurezza e incidenti;
- modalità di assistenza in caso di blocco o malfunzionamento;
- aggiornamenti e correzioni di sicurezza;
- backup e tempi previsti per il ripristino del servizio;
- autenticazione degli utenti e possibilità di utilizzare la MFA;
- registrazione e controllo degli accessi;
- localizzazione dei dati ed eventuali fornitori cloud;
- procedura per comunicare vulnerabilità e incidenti;
- restituzione o cancellazione dei dati alla cessazione del contratto;
- eventuale certificazione ISO/IEC 27001, verificandone validità e perimetro.

Se il fabbricante dichiara di essere **“NIS2 compliant”**, il medico o la struttura possono chiedere una dichiarazione più precisa che indichi:

- se l'organizzazione è stata individuata come soggetto NIS;
- il perimetro aziendale interessato;
- le misure di sicurezza applicate al servizio utilizzato;
- la data e il responsabile della dichiarazione;
- eventuali certificazioni o verifiche indipendenti disponibili.

Non è necessario richiedere documenti tecnici riservati, come il rapporto completo di penetration test. È sufficiente ottenere evidenze proporzionate, ad esempio una dichiarazione formale, una sintesi delle misure adottate, un certificato ISO valido o un questionario di sicurezza compilato.

Buone pratiche per lo studio medico

Anche quando il singolo MMG non rientra direttamente nella NIS2, deve:

- utilizzare account personali e non condivisi;
- attivare la MFA quando disponibile;
- mantenere aggiornati computer e software;
- verificare periodicamente i backup;
- proteggere i dispositivi con antivirus e blocco automatico;
- prestare attenzione a e-mail, link e richieste anomale;
- segnalare immediatamente accessi sospetti, perdita di dati o indisponibilità dei servizi;
- seguire le procedure della ASL o della struttura presso cui opera.

IN SINTESI

Il fabbricante soggetto alla NIS2 deve essere conforme, ma non deve necessariamente ottenere una certificazione. La ISO/IEC 27001 costituisce un elemento positivo, ma non equivale a una “certificazione NIS2”. L'MMG non deve certificare la sicurezza del fornitore: deve verificare che il software sia supportato, aggiornato, protetto e accompagnato da informazioni chiare sulla gestione dei dati, degli incidenti e della continuità del servizio.

Intelligenza artificiale

INTELLIGENZA ARTIFICIALE NELLA PRATICA CLINICA

Tra Europa e Italia, le regole per l’AI in sanità prendono forma: all’AI Act europeo si affianca la Legge italiana n. 132/2025, in vigore dal 10 ottobre 2025 con principi dedicati alla tutela e all’uso dell’intelligenza artificiale in medicina.

Date principali

<i>Data</i>	<i>Cosa cambia</i>
02.02.2025	Obbligo di formare il personale che utilizza sistemi di IA e applicazione dei primi divieti.
02.08.2025	Prime regole per i modelli di IA per finalità generali.
02.08.2026	Applicazione generale dell’AI Act, salvo le scadenze specifiche.
02.12.2027	Applicazione delle regole per determinati sistemi ad alto rischio indicati nell’Allegato III.
02.08.2028	Applicazione delle regole per i sistemi di IA ad alto rischio integrati in prodotti regolamentati, compresi alcuni dispositivi medici.

Cosa devono fare fabbricante e medico

<i>Fabbricante o fornitore</i>	<i>MMG utilizzatore</i>
Deve stabilire il livello di rischio del sistema, documentarne funzionamento e limiti, verificare qualità dei dati, accuratezza, sicurezza informatica e possibilità di supervisione umana. Per l'IA integrata in un dispositivo medico deve coordinare gli obblighi dell'AI Act con quelli dell'MDR.	Deve conoscere finalità e limiti dello strumento, utilizzare dati corretti, valutare criticamente il risultato e segnalare eventuali errori o situazioni pericolose. La decisione clinica finale non può essere delegata automaticamente al sistema.

Non tutte le chatbot o i programmi che utilizzano l'IA sono sistemi ad alto rischio. La classificazione dipende dalla funzione concretamente svolta e, per i dispositivi medici, dal ruolo dell'IA nella sicurezza e nella decisione clinica.

PER L'MMG

Quando l'IA entra nel percorso di cura, la trasparenza e la responsabilità restano in capo al medico. Il paziente va sempre informato in modo chiaro e comprensibile; al tempo stesso, l'MMG mantiene la piena titolarità della decisione finale, con il compito di verificare che l'output dell'IA sia sempre coerente con il quadro clinico complessivo.

Standard

ISO 9001, ISO 27001 E ISO 13485 IN PAROLE SEMPLICI

Le norme ISO attestano la qualità e l'organizzazione dei processi di un'azienda, ma non vanno confuse con la certificazione specifica del singolo software o dispositivo medico.

Standard	Cosa indica	È obbligatorio?
ISO 9001:2026	L'azienda dispone di un sistema organizzato per gestire qualità, processi, clienti e miglioramento continuo.	Generalmente no, salvo richiesta contrattuale o di gara. Non dimostra da sola la conformità MDR del dispositivo.
ISO/IEC 27001:2022	L'azienda gestisce in modo strutturato la sicurezza delle informazioni e i relativi rischi.	Generalmente no. È un elemento positivo, ma non equivale automaticamente alla conformità GDPR o NIS2.
ISO 13485:2016	L'azienda applica un sistema qualità specifico per la progettazione e la gestione dei dispositivi medici.	L'MDR richiede al fabbricante un sistema qualità adeguato, ma non impone in ogni caso il possesso formale del certificato ISO 13485. È comunque lo standard più pertinente per il settore.

Cosa deve controllare l'MMG

Quando il fornitore dichiara di possedere una certificazione ISO, è opportuno verificare:

- che il certificato sia valido e non scaduto;
- quale società e quali sedi comprende;
- quali prodotti, servizi e attività sono inclusi;
- quale organismo lo ha rilasciato;
- che il servizio utilizzato rientri effettivamente nel certificato.

ATTENZIONE

Se il fornitore afferma che “il cloud è certificato ISO 27001”, potrebbe essere certificato soltanto il data center. Questo non significa necessariamente che lo siano anche l'applicazione, l'assistenza e l'intera organizzazione del fabbricante.

IN SINTESI

Le certificazioni ISO sono un utile indice di affidabilità organizzativa, ma l'MMG deve verificare soprattutto la regolarità del dispositivo, la protezione dei dati, la continuità del servizio e la capacità del fornitore di gestire assistenza e incidenti.

FSE 2.0

PATIENT SUMMARY: COSA DEVE AGGIORNARE L'MMG

DM 27 giugno 2025 — GU n. 202 del 1° settembre 2025.

Obbligo e scadenza

Il Profilo sanitario sintetico è redatto e aggiornato dal MMG/PLS. Il decreto richiede alle Regioni e Province autonome di garantirne la redazione su tutto il territorio entro il **30 settembre 2025**. L'effettiva modalità tecnica dipende dal sistema regionale, ma il compito professionale non va confuso con un target commerciale o contrattuale locale.

Contenuti e responsabilità

<i>Dato</i>	<i>Regola pratica</i>
Identità e contatti del medico	Dati obbligatori secondo tracciato.
Problemi clinici rilevanti / cronici	Inserire e mantenere informazioni utili alla continuità; evitare sovraccarico irrilevante.
Allergie e reazioni avverse	Distinguere farmaci, alimenti, sostanze e veleno di insetti; verificare l'aggiornamento.
Terapie croniche	Verificare completezza e coerenza delle prescrizioni attribuite al MMG/PLS.
Trapianti, organi mancanti, malformazioni rilevanti	Compilare quando pertinente e clinicamente significativo.
Dati precompilati da ANA/EDS	Il sistema può valorizzarli automaticamente, ma il medico deve verificarli nei casi previsti.
Dati facoltativi	Ad esempio: caregiver e ausili, secondo specifiche; usare minimizzazione e pertinenza.

Come gestirlo nella pratica

- Il Patient Summary va aggiornato quando cambia un'informazione importante: nuova diagnosi, terapia cronica, allergia, dimissione ospedaliera o nuova presa in carico.
- Prima di confermare il documento, il medico deve confrontare i dati con la cartella, le prescrizioni e i referti, correggendo eventuali incongruenze.
- L'aggiornamento deve rimanere tracciabile e rispettare le regole del Fascicolo sanitario elettronico, comprese quelle sull'accesso e sull'oscuramento.
- Il Patient Summary è una sintesi destinata alla continuità delle cure: non sostituisce la cartella clinica completa né la valutazione diretta del paziente.

Flussi informativi

SIAP: COSA VIENE RICHIESTO AL MEDICO

DM 4 agosto 2025 — GU n. 202 del 1° settembre 2025.

Chi trasmette cosa

La catena dell'informazione sanitaria si basa su ruoli ben distinti: l'MMG e il PLS adempiono agli obblighi informativi registrando i dati tramite software interoperabili; la trasmissione istituzionale verso SIAP e NSIS spetta invece a Regioni e Province Autonome. Il compito primario del medico resta quindi garantire un'alimentazione del dato precisa e tempestiva alla fonte.

Cadenza

Periodo	Trasmissione al NSIS
Attività dal gennaio 2026	Nel 2026: aggregazione mensile e invio entro il mese successivo, secondo specifiche.
Dal 1° gennaio 2027	Cadenza settimanale, entro la settimana successiva.

Come preparare lo studio e la cartella clinica

- Mantenere aggiornate anagrafiche, diagnosi, problemi clinici, prescrizioni e prestazioni, evitando duplicazioni e descrizioni ambigue.
- Aggiornare il software alla versione compatibile con le specifiche regionali; deve rendere comprensibili ricevute, errori e invii rimasti in coda.
- Riconoscere un dato incompleto o non plausibile e correggerlo mantenendo traccia dell'operazione.
- Far transitare i dati soltanto attraverso i canali autorizzati: non creare archivi paralleli o esportazioni non necessarie.
- In caso di indisponibilità, sapere come continuare l'attività e come recuperare gli invii quando il servizio torna operativo.

Obbligo del fornitore

Implementare tracciati e controlli senza alterare la semantica clinica; documentare versioni, test e mapping; proteggere canali e credenziali; restituire esiti leggibili; assistere il medico nella correzione. La “conformità SIAP” va provata per Regione e versione e non può essere dichiarata in astratto.

ICD-10-IM

ICD-10-IM: LA TRANSIZIONE ALLA NUOVA CLASSIFICAZIONE

La nuova classificazione delle diagnosi, affiancata dalla CIPI, è stata introdotta con il DM 23 ottobre 2025.

CHE COSA CAMBIA

L'ICD-10-IM, insieme alla classificazione CIPI, diventa obbligatoria nei flussi NSIS interessati dal 1° gennaio 2027, dopo una fase di sperimentazione nel corso del 2026.

Il fornitore di software clinico deve aggiornare classificazioni e mappature quando queste funzioni rientrano nel prodotto o nel contratto, preservando la tracciabilità dei codici storici; non si tratta di un obbligo generale di certificazione MDR.

IN PRATICA, PER L'MMG

Per il medico significa prepararsi alla nuova codifica e alla relativa formazione, in coordinamento con Regione e fornitore del software, man mano che si avvicina l'avvio obbligatorio del 1° gennaio 2027.

Sanzioni

SANZIONI: I PRINCIPALI RISCHI

Gli importi indicati sono le fasce o i massimali previsti dalla legge: la sanzione non viene applicata automaticamente nella misura massima. L'autorità valuta gravità, durata, conseguenze, comportamento del soggetto e misure adottate.

Norma	Caso principale	Sanzione prevista
MDR	L'MMG o il referente incaricato non segnala un incidente grave relativo a un dispositivo medico. L'incidente grave, anche solo sospetto, deve essere segnalato entro dieci giorni.	Da 26.000 a 120.000 euro.
MDR	Il fabbricante non segnala o non indaga gli incidenti e non adotta le necessarie azioni correttive.	Da 24.200 a 145.000 euro.
MDR	Viene commercializzato o messo in servizio un dispositivo non conforme.	Da 24.200 a 145.000 euro, salvo che il fatto costituisca reato.
GDPR	Mancano adeguate misure di sicurezza, registri, contratti o controlli organizzativi.	Fino a 10 milioni di euro o al 2% del fatturato mondiale.
GDPR	Sono violati principi, basi giuridiche o diritti del paziente.	Fino a 20 milioni di euro o al 4% del fatturato mondiale.

16 Sanzioni

Norma	Caso principale	Sanzione prevista
NIS2	Un soggetto NIS non rispetta gli obblighi di sicurezza, governance o notifica.	Fino a 10 milioni o al 2% per i soggetti essenziali; fino a 7 milioni o all'1,4% per quelli importanti.
AI Act	Il fornitore o l'utilizzatore viola gli obblighi applicabili al sistema di IA.	Importo variabile in base alla violazione, al ruolo e alle dimensioni del soggetto.
Norme ISO	L'organizzazione non possiede una certificazione non richiesta dalla legge.	Nessuna sanzione diretta, salvo conseguenze previste da contratti, gare o capitolati.
Patient Summary, SIAP e ICD	Mancato adempimento degli obblighi professionali o informativi.	Non esiste una sanzione unica: possono derivare conseguenze professionali, organizzative, convenzionali o privacy.

COSA DEVE RICORDARE L'MMG

Un singolo evento può coinvolgere contemporaneamente più normative. Ad esempio, un software medico che si blocca e rende visibili dati sanitari a persone non autorizzate può richiedere:

- la segnalazione dell'incidente relativo al dispositivo;
- la gestione del data breach GDPR;
- l'eventuale notifica NIS2 da parte del soggetto obbligato;
- la comunicazione al fabbricante e alla struttura sanitaria.

IN PRATICA

L'MMG non deve stabilire da solo quale normativa applicare. Deve segnalare immediatamente l'evento attraverso i canali previsti, conservare le informazioni utili e fornire una descrizione completa e coerente dell'accaduto.

17.1

Stato aziendale

MILLENNIUM: UN SISTEMA DI COMPLIANCE STRUTTURATO

Il quadro completo dei presidi attivi e delle tempistiche di adeguamento ad oggi.

Ambito	Stato	Evidenza disponibile	Verifica / azione richiesta
MDR - Millengine	Percorso avanzato	Valutazione di conformità classe IIa avviata con KIWA (NB 0476). Contratto del 15.05.2024, fascicolo trasmesso il 28.02.2025, Confirmation Letter CERBO0219224 Rev.1.	Proseguire il confronto con l'organismo notificato e preparare in parallelo dichiarazione UE, UDI, registrazioni e sorveglianza post-market.
Millewin e Milleweb	Presidiato	Prodotti registrati come dispositivi di classe I secondo il quadro applicabile; l'evoluzione del modulo Millengine è ricompresa nel programma MDR di classe IIa.	Mantenere aggiornata, per ciascun modulo e versione, la matrice che collega destinazione d'uso, classe, documenti e stato regolatorio.
Sistema qualità e ISO 13485	Strutturato	Sistema qualità integrato, PRRC, fascicolo tecnico e interlocuzione con l'organismo notificato già operativi.	Consolidare audit, CAPA, controllo fornitori, PMS/PMCF, ciclo di vita software e gestione delle modifiche.

17.1 Stato aziendale

Ambito	Stato	Evidenza disponibile	Verifica / azione richiesta
ISO 9001	Presidiato	I processi aziendali sono governati attraverso il Sistema di gestione integrato e le relative procedure.	Presentare sempre certificato vigente, perimetro e sedi interessate e pianificare la transizione alla nuova edizione quando applicabile.
ISO/IEC 27001	In evoluzione	I controlli di sicurezza sono sviluppati nel programma NIS2 e nel percorso di cybersecurity del dispositivo medico.	Proseguire l'integrazione in un ISMS coerente con ISO/IEC 27001, definendone formalmente perimetro, rischi e dichiarazione di applicabilità.

Millennium gestisce la compliance come un processo continuo: requisiti, prodotti, versioni ed evidenze vengono ricondotti a responsabilità definite e a piani di aggiornamento verificabili.

17.2

Stato aziendale

MILLENNIUM: PROTEZIONE DEI DATI, SICUREZZA E INTELLIGENZA ARTIFICIALE

I presidi organizzativi già operativi e i prossimi passi per consolidarli.

Ambito	Stato	Evidenza disponibile	Verifica / azione richiesta
GDPR	Presidiato	Presidi privacy operativi per i servizi sanitari e gestione continuativa dei trattamenti di dati sulla salute.	Proseguire l'aggiornamento di registro, DPIA, accordi art. 28, sub-responsabili, conservazione, log e prove di gestione del data breach.
NIS2	Percorso avanzato	Programma di adeguamento in fase avanzata, con adempimenti ACN già completati in parte e misure integrate nei processi di sicurezza.	Completare la mappatura delle misure applicabili, le evidenze di governance, la supply chain e le prove di notifica degli incidenti.
Cybersecurity MDR	Integrato	La sicurezza è trattata nel ciclo di vita di Millengine, nella gestione dei rischi e nelle attività di verifica e penetration test.	Mantenere allineati risk file, dipendenze software, vulnerabilità, patch, PMS e comunicazioni agli utilizzatori.

17.2 Stato aziendale

Ambito	Stato	Evidenza disponibile	Verifica / azione richiesta
AI Act	Adeguamento attivo	Le funzionalità DSS e algoritmiche sono ricomprese nella governance di prodotto e nella formazione degli utilizzatori.	Completare inventario IA, ruoli, classificazione, qualità dati, logging, supervisione umana e controllo delle modifiche.
Legge 132/2025	Presidiato	L'impostazione del prodotto mantiene la decisione finale in capo al medico e utilizza il software come supporto professionale.	Rendere sempre chiari finalità, limiti, verifiche periodiche e modalità con cui il medico può valutare o non seguire il suggerimento.

17.3

Stato aziendale

MILLENNIUM: SERVIZI PER LA MEDICINA GENERALE

Una Roadmap prodotto allineata alle nuove disposizioni nazionali e regionali.

Ambito	Stato	Evidenza disponibile	Verifica / azione richiesta
Patient Summary	Sviluppo attivo	Funzionalità inserite nella roadmap di prodotto e nei programmi di aggiornamento per la medicina generale.	Consolidare i test sui tracciati nazionali e regionali, precompilazione, verifica, audit trail, oscuramenti e gestione degli errori.
SIAP	Sviluppo attivo	Adeguamenti applicativi programmati per supportare i nuovi flussi dell'assistenza primaria.	Documentare la matrice Regione-versione, i test end-to-end, ricevute e scarti, continuità e passaggio dalla cadenza mensile a quella settimanale.
ICD-10-IM	Transizione pianificata	Preparazione della nuova classificazione e delle relative mappature applicative.	Allineare dizionari e comunicazione alla sperimentazione 2026 e all'avvio NSIS dal 01.01.2027, preservando la tracciabilità dei codici storici.
Formazione MMG	Presidiato	Materiali informativi, assistenza e accompagnamento degli utilizzatori già presenti.	Integrare in un percorso unico MDR, incidenti, Patient Summary, SIAP, ICD-10, privacy, cybersecurity e uso responsabile dell'IA.

POSIZIONAMENTO COMPLESSIVO

Millennium dispone di un sistema di compliance integrato che presidia qualità, regolamentazione dei dispositivi medici, protezione dei dati e sicurezza informatica. Il percorso MDR di Millengine è nella fase formale di valutazione con l'organismo notificato, mentre i servizi destinati alla medicina generale vengono aggiornati secondo le scadenze nazionali e le specifiche regionali. L'azienda può quindi presentarsi come organizzazione con compliance strutturata e in continuo adeguamento, descrivendo per ogni prodotto il relativo stato e le evidenze disponibili.

Fonti

FONTI UFFICIALI ESSENZIALI

Per approfondire, sempre sui testi originali e sulle pagine istituzionali, che possono essere aggiornate nel tempo.

- **MDR — Regolamento (UE) 2017/745, testo consolidato**
eur-lex.europa.eu/eli/reg/2017/745
- **Regolamento (UE) 2023/607 — transizioni MDR/IVDR**
eur-lex.europa.eu/eli/reg/2023/607/oj
- **D.Lgs. 5 agosto 2022, n. 137 — adeguamento nazionale MDR e sanzioni**
www.gazzettaufficiale.it/eli/id/2022/09/13/22G00145/sg
- **Ministero della Salute — dispositivo-vigilanza e segnalazioni**
www.salute.gov.it/new/it/tema/dispositivi-medici/vigilanza-sugli-incidenti/
- **DM 1 luglio 2025 — termini e modalità di segnalazione incidenti DM**
www.gazzettaufficiale.it/eli/id/2025/09/19/25A05071/SG
- **Commissione europea — MDCG 2019-11 rev.1, software qualification/ classification**
health.ec.europa.eu/latest-updates/update-mdcg-2019-11-rev1-qualification-and-classification-software-regulation-eu-2017745-and-2025-06-17_en
- **GDPR — Regolamento (UE) 2016/679**
eur-lex.europa.eu/eli/reg/2016/679/oj

Fonti

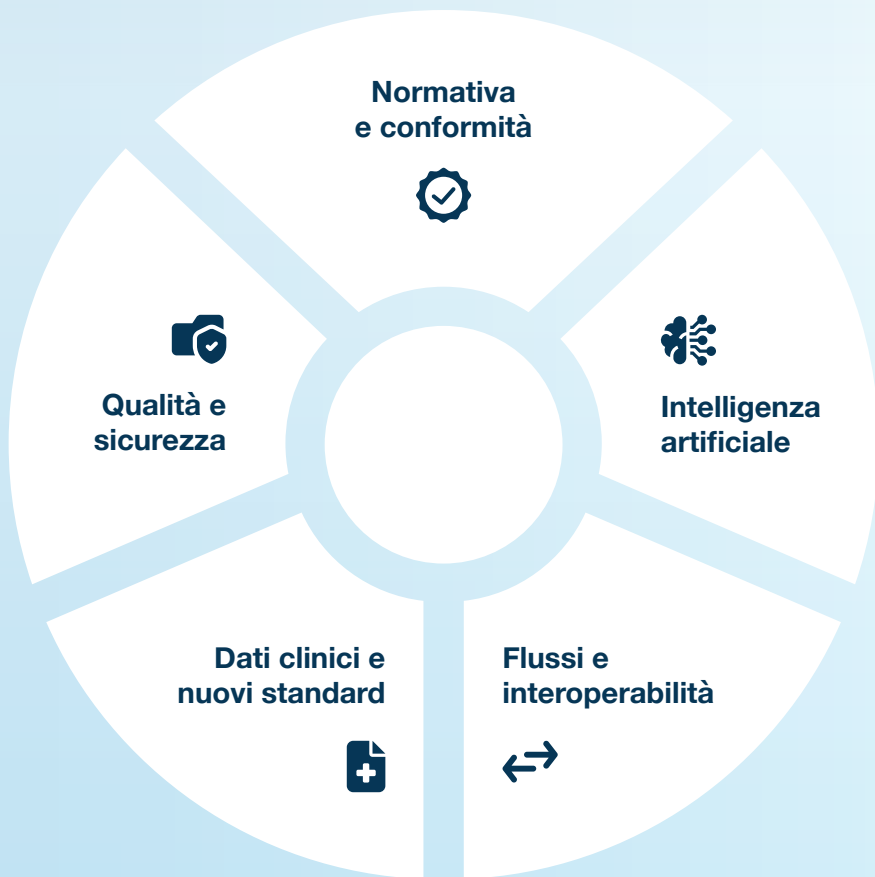
- **Garante — chiarimenti sull'applicazione della disciplina per finalità di cura**
www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942
- **Garante — FAQ Fascicolo sanitario elettronico**
www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/fascicolo-sanitario-elettronico
- **Direttiva (UE) 2022/2555 — NIS2**
eur-lex.europa.eu/eli/dir/2022/2555/oj
- **D.Lgs. 4 settembre 2024, n. 138 — recepimento NIS2**
www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG
- **ACN — portale e adempimenti NIS**
www.acn.gov.it/portale/nis

Fonti ufficiali: salute digitale, IA e standard

- **AI Act — Regolamento (UE) 2024/1689**
eur-lex.europa.eu/eli/reg/2024/1689/oj
- **Commissione europea — AI Act, calendario aggiornato 2026**
digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- **Legge 23 settembre 2025, n. 132 — intelligenza artificiale**
www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/SG

Fonti

- **DM 27 giugno 2025 — Profilo sanitario sintetico (GU 01.09.2025)**
www.gazzettaufficiale.it/eli/id/2025/09/01/25A04814/SG
- **DM 4 agosto 2025 — SIAP (GU 01.09.2025)**
www.gazzettaufficiale.it/eli/id/2025/09/01/25A04813/SG
- **DM 23 ottobre 2025 — ICD-10-IM e CIPI**
www.gazzettaufficiale.it/eli/id/2025/12/10/25A06571/SG
- **Ministero della Salute — classificazione ICD-10-IM**
www.salute.gov.it/new/it/tema/assistenza-ospedaliera-sdo/la-classificazione-delle-diagnosi-icd-10-im/
- **ISO — ISO 9001:2026**
www.iso.org/standard/9001
- **ISO — ISO/IEC 27001:2022**
www.iso.org/standard/27001
- **Ministero della Salute — classificazione dei dispositivi medici**
www.salute.gov.it/new/it/tema/dispositivi-medici/classificazione-nazionale-dispositivi-medici-cnd/
- **Commissione europea — documenti MDCG e guidance**
health.ec.europa.eu/medical-devices-sector/new-regulations/guidance-mdcg-endorsed-documents-and-other-guidance_en



Con il contributo di Millennium