GDPR INSIGHT

SERIES

SANITÀ DIGITALE E TELEMEDICINA

PRIVACY, CYBERSICUREZZA E INTELLIGENZA ARTIFICIALE NELLA SANITÀ DIGITALE

NETPATROL

DATA PROTECTION & CYBER SECURITY

NET PATROL ITALIA

Net Patrol Italia è una società di consulenza specializzata in **privacy** e **cybersecurity**.

Net Patrol raccoglie il **know-how** di professionisti operanti da anni nel settore della privacy, cybersecurity e ICT.

La nostra squadra, formata da **esperti di data protection, avvocati e tecnici specializzati**, affianca da vicino il cliente per sviluppare o migliorare i sistemi di gestione aziendali per privacy e cybersecurity.

Il nostro obiettivo è quello di dare al cliente un **interlocutore unico,** in grado di affrontare la protezione dei dati con approccio multidisciplinare e **business oriented**.

Crediamo fermamente che privacy e cybersecurity siano due pilastri importanti dell'economia **data-driven**, oltre che un mezzo per valorizzare il proprio business.

- Privacy law
- Data Protection Officer
- Cybersecurity & Cyber law advisory

PARTNERSHIP

intercom SOLUTIONS

ATMAN

karmasec

SANITÀ 4.0 – IL FUTURO DELLA MEDICINA È DIGITALE

Quasi il **50% delle aziende sanitarie** italiane stima un aumento degli investimenti in sanità digitale nei prossimi mesi. Nell'ultimo periodo le attività di tele-monitoraggio sono aumentate del 37% e le televisite del 35%.

Secondo l'**Health Report 2020** del gruppo Stada, almeno il 40% dei cittadini europei sarebbero già disposti ad usare app per la salute, ad esempio per comunicare automaticamente dati al proprio medico curante.

L'evoluzione della medicina non può però limitarsi agli investimenti tecnologici. La tecnologia deve essere governata e gestita, oltre che **sicura** e pienamente rispettosa della normativa **privacy**.

"Giuro di rispettare il segreto professionale e di tutelare la riservatezza su tutto ciò che mi è confidato, che osservo o che ho osservato, inteso o intuito nella mia professione o in ragione del mio stato o ufficio"

Un nuovo paradigma

La medicina digitale va ben oltre la semplice **telemedicina**, cioè l'insieme di tecniche mediche e informatiche che permettono la fruizione di servizi sanitari a distanza.

Con la diffusione dell'intelligenza artificiale e delle sue tecnologie abilitanti, come 5G, Big Data, app e sistemi connessi, è più corretto parlare di "**connected care**".

La connected care non è semplice telemedicina, ma un sistema sanitario connesso e interconnesso, capace di offrire ai pazienti un'esperienza di cura condivisa, pienamente personalizzata, e senza soluzione di continuità.

Un vero e proprio **cambio di paradigma**, dove la persona è al centro di una costellazione di sistemi digitalizzati e interconnessi; regolati da modelli organizzativi che favoriscono l'integrazione e l'efficienza delle cure a livello nazionale e locale, anche grazie alle nuove tecnologie.

Salute data-driven, tra privacy e cybersecurity

Connected care e industria 4.0 hanno alcuni fattori in comune: **digitalizzazione** e processi **data-driven**.

Dove ci sono dati personali e processi digitali, non può certo mancare grande attenzione a **privacy** e **cybersecurity**, che nella connected care diventano veri e propri pilastri portanti.

Vedremo insieme come privacy e cybersecurity interagiscono con il mondo della sanità digitale, e per quale motivo sono due fattori essenziali, al pari dell'investimento tecnologico.

Connected care e Mobile health

La connected care è un fenomeno che abbraccia a 360 gradi amministrazione pubblica, aziende, e persone.

La persona è al centro di innumerevoli servizi digitali connessi, talvolta destinati esclusivamente al mercato consumer, ma che comunque partecipano all'ecosistema della connected care.

Il panorama è quello di una moltitudine di servizi e app che abilitano una nuova gestione della cura dallo smartphone: la **mobile health**.

A questi servizi fanno capo una moltitudine di soggetti facenti parti della **filiera del trattamento di dati**, che si fondono insieme per garantire la sicurezza dei dati e conformità del trattamento in ogni fase.

Il ruolo dell'intelligenza artificiale

Come vedremo meglio, l'intelligenza artificiale, e in particolare il machine learning, ricopriranno un ruolo sempre più centrale anche nella sanità.

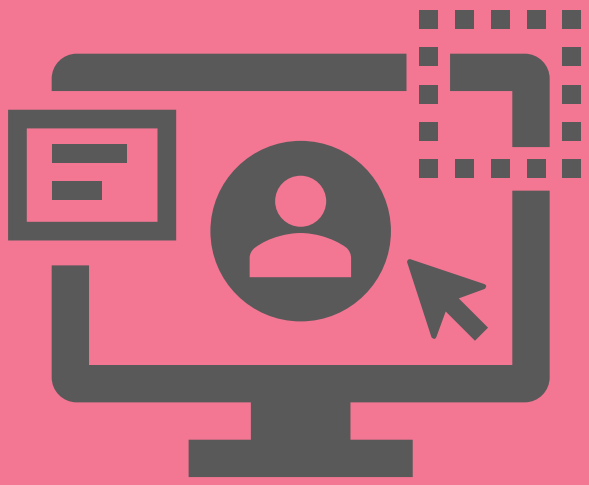
Per certi versi, l'intelligenza artificiale potrà aiutare i medici ad essere **più umani** – automatizzando molte attività che oggi richiedono attenzione umana.

Ma anche in questo caso sarà fondamentale prestare attenzione alla privacy, intesa come trattamento lecito, trasparente ed etico dei dati.

D'altronde, questi sono già elementi fondamentali della professione medica.

FASCICOLO SANITARIO ELETTRONICO E TELEMEDICINA

FUNZIONAMENTO, FINALITÀ E ACCESSO



FASCICOLO SANITARIO ELETTRONICO E SISTEMI DI SORVEGLIANZA SANITARIA

Il Fascicolo Sanitario Elettronico è stato istituito con il D.L. 179/2012, coordinato con la legge di conversione 221/2012.

"Il Fascicolo Sanitario Elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito. Il FSE è istituito nel rispetto della normativa vigente in materia di protezione dei dati personali [...]"

Nella definizione del FSE il legislatore ha voluto dare fin da subito grande attenzione alla normativa per la protezione dei dati personali, tanto che è la legge stessa a definire le finalità del trattamento e le condizioni di legittimità.

Finalità del FSE e liceità del trattamento

Il FSE è istituito dalle Regioni e dalle province autonome per perseguire le seguenti finalità:

	Prevenzione, diagnosi, cura e riabilitazione
	Studio e ricerca scientifica in campo medico, biomedico ed epidemiologico
	Programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria

Come appare evidente, delle tre finalità, soltanto la prima è rivolta alla cura del cittadino.

Le rimanenti due riguardano invece la **gestione della sanità pubblica**, sia nella sua accezione di ricerca e sviluppo, che per quanto riguarda la governance nazionale del sistema sanitario.

Condizioni di liceità del trattamento

Fino al 2020 la condizione di liceità per l'attivazione e alimentazione del FSE era il **consenso** del cittadino.

Il D.L. 34/2020 (emergenza COVID-19) ha però, **abrogato** l'art. 3-bis del D.L. 179/2012, che prevedeva il consenso come condizione di liceità, cambiando drasticamente direzione.

A seguito di questa abrogazione, si deve ritenere che la creazione del FSE e la successiva alimentazione continuativa di dati debba trovare la sua **condizione di liceità** nella legge stessa; non più nel consenso dell'interessato.

Il **Regolamento Generale sulla Protezione dei dati Personali** (GDPR) prevede due specifiche condizioni di liceità che possono rientrare nella fattispecie del FSE:

Art. 9(2) lett. h)	Strumento necessario per finalità di medicina preventiva, **diagnosi**, assistenza, **terapia sanitaria** o gestione dei servizi e sistemi sanitari.
Art. 9(2) lett. i)	Strumento necessario per la protezione da **gravi minacce** per la salute a carattere transfrontaliero (epidemia e pandemia COVID-19).

Accesso al FSE

La legge prevede tre categorie di soggetti che possono avere accesso al FSE:

	L'assistito, che può consultare sia i propri dati sanitari che amministrativi
	Esercenti professioni sanitarie, sia pubblici che privati, compreso il medico di base
	Il Ministero della salute, le Regioni e le province autonome

L'accesso al FSE può avvenire esclusivamente previo **consenso** del soggetto interessato, che deve essere **gestito** nel rispetto degli articoli 6 e 7 del **GDPR**.

Chiaramente, la normativa privacy non è mai d'intralcio alla sanità. Per questo, sia il D.L. 179/2012 che il GDPR, prevedono la possibilità di accedere al FSE nel caso in cui il paziente non sia in condizioni di prestare il suo consenso, ma l'accesso sia necessario per **salvaguardare la sua vita** o quella di terzi.

Quali dati confluiscono nel FSE?

Nel FSE confluiscono sia dati sanitari che amministrativi riferibili all'assistito.

In particolare, il FSE è popolato da dati che riguardano terapie, anamnesi, prescrizioni di medicinali e visite specialistiche, prescrizioni di esami di laboratorio e referti di laboratorio, referti radiologici, verbali, e così via.

Nel FSE è inoltre presente il **patient summary**, di competenza del medico di base, che contiene i dati necessari a gestire un'emergenza sanitaria.

In ogni caso l'assistito ha sempre il **diritto** di ottenere tutte le informazioni circa i dati trattati e gli accessi effettuati al FSE, come previsto sia dal GDPR che dalla normativa italiana.

Il FSE come fulcro della nuova connected care

Il FSE viene alimentato continuativamente da una moltitudine di soggetti e di dati personali. La normativa prevede che tutti i soggetti autorizzati possono popolare di dati il FSE, anche al di fuori della Regione di appartenenza dell'assistito.

Le informazioni lì contenute devono essere rese **interoperabili**, per consentire la consultazione e l'utilizzo da parte di tutti i soggetti coinvolti a livello locale e nazionale.

Per questo motivo il FSE potrà essere il vero e proprio fulcro della connected care italiana – un nodo di aggregazione e condivisione di dati, documenti, analisi e statistiche.

L'attuazione del FSE in Italia

Il FSE non è ancora operativo in tutte le regioni italiane. Secondo gli ultimi aggiornamenti (marzo 2020) risulta operativo su 14 regioni su 20.

Per quanto riguarda invece l'interoperabilità del FSE, nodo fondamentale per la sanità digitale, risultano operative 12 regioni.

Per i cittadini i dati non sono entusiasmanti. A marzo 2020 **solo il 23%** dei cittadini aveva attivato il FSE. Un dato destinato comunque a cambiare anche grazie alle modifiche portate dal D.L. 34/2020.

PRIVACY E TELEMEDICINA

REQUISITI NORMATIVI E ACCORDO STATO-REGIONI

IL TRATTAMENTO DI DATI SULLA SALUTE

Nel 2016 è entrato in vigore il Regolamento Generale sulla protezione dei dati ("**GDPR**"). Il Regolamento **vieta** il trattamento di **categorie particolari** di dati personali (come quelli sulla salute), salvo che per alcune eccezioni – previste dall'articolo 9.

I dati sulla salute, genetici, e biometrici, possono essere trattati soltanto in ragione di **specifiche condizioni di liceità**. Nei prossimi paragrafi vedremo quali sono i principali requisiti normativi da rispettare per evitare di incorrere in gravi sanzioni.

I servizi di telemedicina sono stati disciplinati con **Accordo Stato – Regioni sulla telemedicina del 17 novembre 2020**, con specifici obblighi e responsabilità per gli operatori sanitari, in materia di privacy e cybersicurezza.

Condizioni di liceità del trattamento in ambito sanitario

Il trattamento di dati sulla salute in ambito sanitario può essere principalmente realizzato sulla base di **tre principali condizioni di liceità**, previste dall'articolo 9 del GDPR.

	Motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.
	Motivi di interesse pubblico nel settore della sanità pubblica (come la gestione di emergenze sanitarie nazionali).
	Trattamento necessario a finalità di medicina preventiva, diagnosi, assistenza, terapia sanitaria o sociale o gestione dei servizi sanitari o sociali.

Moltissime strutture sanitarie, sia pubbliche che private, ancora fondano la liceità di trattamenti di dati in ambito sanitario sulla base del **consenso** del soggetto interessato.

Questa prassi deriva dalla **precedente normativa** (D.Lgs 196/2003, Codice Privacy) che prevedeva il consenso come primaria condizioni di liceità del trattamento.

Ai sensi dell'articolo 75 del Codice novellato il **consenso non è più necessario** per il trattamento dei dati in ambito sanitario.

Se non l'hai già fatto, aggiorna i processi aziendali per essere conformi alle nuove basi giuridiche.

Quando è necessario il consenso?

L'esistenza di condizioni di liceità diverse dal consenso per il trattamento di dati relativi alla salute non deve trarre in inganno.

Rimangono alcuni casi in cui questi dati possono essere trattati **esclusivamente con il consenso** della persona, come:

	Utilizzo di app mediche, o app e servizi che comunque trattano anche dati sulla salute
	Servizi accessori, come programmi di fidelizzazione per la clientela (es. farmacie o cliniche private)
	Accesso al FSE
	Consegna del referto online

Per comprendere quando è necessario il consenso e quando invece devono essere usate diverse condizioni di liceità sarà necessario **esaminare** lo specifico trattamento di dati e valutare caso per caso.

Trasparenza del trattamento

Il **Titolare del trattamento**, cioè il soggetto che tratta dati personali nel perseguimento delle proprie finalità, è tenuto a fornire tutte le **informazioni** necessarie ai soggetti interessati.

Queste informazioni devono essere rese con **linguaggio semplice e chiaro**.

L'accordo Stato-Regioni prevede **specifici oneri informativi** ai pazienti di servizi di telemedicina. Tra i principali elementi obbligatori:

1	Descrizione della gestione dei dati, dei soggetti che hanno accesso
2	Descrizione dei compiti delle strutture coinvolte
3	Elenco aggiornato dei Responsabili del trattamento
4	Diritti dell'assistito e modalità di contatto

A questi oneri informativi devono aggiungersi quelli già previsti dal **GDPR** e dagli **App Store** (in particolare Apple Store, che dall'8 dicembre 2020 prevede specifiche misure di trasparenza sui dati).

Data retention

La definizione delle politiche di data retention per quanto riguarda i dati sanitari dipende in parte dalla normativa di settore, che prevede numerosi e differenziati **tempi di conservazione** per la documentazione sanitaria.

Ad esempio:

5 anni	Certificato di idoneità sportiva
10 anni	Documentazione iconografica radiologica
∞	Cartelle cliniche, esami di laboratorio, referti

Nel caso in cui la conservazione della documentazione non sia disciplinata dalla legge, spetta al singolo Titolare del trattamento **definire le politiche di data retention**, nel rispetto dell'articolo 5 GDPR.

Ad esempio, le cliniche non convenzionate dovranno definire autonomamente i tempi di conservazione delle cartelle cliniche dei pazienti.

Privacy by design

La telemedicina è un universo fatto di **prodotti** e **servizi digitali** di ogni tipo.

La normativa (GDPR) prevede che questi prodotti e servizi digitali siano in grado di garantire la piena **conformità** del trattamento di dati ai requisiti di legge.

*I software ed i dispositivi che entrano nel mercato della sanità digitale, dovrebbero essere sviluppati secondo il principio di **privacy by design**, come previsto dall'articolo 25 del GDPR.*

La creazione di prodotti rispettosi della privacy by design richiede una vera e propria integrazione del **ciclo di sviluppo** dei prodotti.

Ecco alcuni dei criteri da seguire:

1	La documentazione tecnica identifica i requisiti privacy che saranno implementati e verificati nelle successive fasi di sviluppo.
2	Il software è sviluppato con caratteristiche di "somma positiva", limitando trade-off non necessari tra privacy e funzionalità.
3	Tutte le impostazioni di default del software sono a favore della privacy dell'utente.
4	Il trattamento di dati effettuato dal software è compatibile e rispetta i requisiti legali di riferimento e le politiche di protezione dei dati delle aziende che lo adottano.

Privacy by design e responsabilità professionale

Il requisito di privacy by design non si applica solo allo sviluppo di software, ma anche ai **processi organizzativi** che regolano le prestazioni di telemedicina.

Tutte le attività di trattamento dati devono essere realizzate nel rispetto della normativa.

*L'accordo Stato-Regioni prevede la **responsabilità professionale** dei sanitari degli atti condotti nell'esercizio dei servizi di telemedicina.*

I sanitari, e le strutture che offrono servizi di telemedicina, hanno il dovere di **gestire i rischi** derivanti anche dal trattamento di dati personali dei pazienti, scegliendo le soluzioni operative che offrano le migliori **garanzie** di proporzionalità, appropriatezza, efficacia, **sicurezza**, e **rispetto dei diritti** della persona.

In caso di danni, sarà quindi onere del sanitario dimostrare di aver scelto soluzioni adeguate a garantire la sicurezza dei dati e dei diritti dei pazienti.

Il GDPR prevede anche una responsabilità in solido caso di violazione di legge da parte dei soggetti coinvolti nel trattamento di dati.

*I soggetti che fanno parte della stessa filiera del trattamento di dati **rispondono in solido** in caso di violazioni di legge o in caso di danno derivante da una violazione di dati.*

Gli operatori di telemedicina dovrebbero quindi **scegliere fornitori** in grado di offrire determinate garanzie, per evitare responsabilità derivanti dalla negligenza di terzi.

Anche i bandi di gara verso la privacy by design

Anche le gare pubbliche nel settore sanitario saranno adeguate ai nuovi standard di conformità privacy del mercato europeo.

I bandi riguardanti l'acquisto di apparecchiature e dispositivi medici saranno infatti modificati per renderli conformi alla normativa privacy e assicurare maggiori tutele per i dati delle persone.

L'**Autorità Garante per la Protezione dei Dati** sta lavorando insieme al **Consip** per integrare i bandi con specifiche misure aggiuntive, come:

- ✓ Impossibilità di accedere, di default, ai dati dei pazienti per il fornitore che esegue attività di assistenza e manutenzione da remoto
- ✓ Qualificazione del fornitore dei dispositivi come **Responsabile del trattamento** (articolo 28 GDPR)
- ✓ Introduzione di specifiche clausole contrattuali per lo sviluppo di software e apparecchiature nel rispetto dei principi di privacy by design e by default

Queste novità non devono stupire, ed anzi devono ritenersi integrazioni doverose per adeguare il mercato interno della sanità alla normativa europea.

Data Protection Officer, mi serve?

Il Data Protection Officer (DPO) è la nuova figura istituita nel 2016 dal GDPR.

Le funzioni del DPO sono principalmente:

	Fornire consulenza in merito al trattamento dei dati personali
	Sorvegliare sull'osservanza della normativa
	Valutare i rischi legati al trattamento di dati

Il DPO può essere incaricato internamente all'organizzazione, o può essere un servizio in outsourcing.

In alcuni casi avere un DPO è **obbligatorio**:

- ✓ Per le amministrazioni pubbliche, come enti, scuole, ospedali
- ✓ Quando viene effettuato un trattamento di categorie particolari (es. dati sulla salute) su larga scala

La valutazione del rischio privacy

C'è un motivo se il giuramento di Ippocrate prevede uno specifico passaggio sulla riservatezza delle informazioni.

I dati sullo stato di salute, così come quelli biometrici o genetici, sono estremamente sensibili.

La normativa privacy riconosce la **pericolosità** di questa tipologia di dati, e per questo motivo sono previsti specifici obblighi per la **valutazione dei rischi** in capo ai titolari e responsabili del trattamento.

Prima di iniziare un trattamento di dati che possa presentare un rischio elevato per le persone, il titolare del trattamento deve svolgere una **valutazione d'impatto** ai sensi dell'articolo 35.

La valutazione d'impatto deve coprire almeno i seguenti macro-argomenti:

	Una descrizione sistematica dei trattamenti, delle finalità, e delle condizioni di liceità
	Una valutazione della necessità e proporzionalità del trattamento
	Una valutazione dei rischi per i diritti e libertà delle persone
	Una valutazione dei rischi derivanti dal trasferimento di dati in paesi extra-UE
	Le misure previste per affrontare i rischi identificati

La valutazione d'impatto è un processo che richiede **particolari competenze** e risorse.

Per questo, è preferibile ottenere l'aiuto di esperti privacy o del proprio DPO, che oltre a sorvegliarne lo svolgimento potrà anche fornire un parere in merito alla valutazione.

In ogni caso è preferibile **integrare** la valutazione d'impatto all'interno dei processi aziendali, per evitare inutili perdite di tempo. Prima di iniziare una nuova attività, ricorda sempre di valutare i rischi privacy.

Non solo privacy, ma anche (cyber)sicurezza

Il Regolamento Generale sulla protezione dei dati ("GDPR") si occupa anche della **sicurezza dei dati** trattati.

In assenza di adeguate misure di sicurezza il trattamento si ritiene **illecito**, esponendo l'azienda a sanzioni amministrative.

Come si valuta l'adeguatezza della sicurezza? Anche in questo caso, è una questione di **valutazione dei rischi**, che variano in base al contesto e anche in base alla tipologia di dati trattati.

È comunque particolarmente importante valutare almeno questi tre parametri:

	Capacità di assicurare su base permanente la riservatezza, integrità e disponibilità dei dati, oltre che la resilienza dei sistemi di trattamento
	Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente
	Capacità di verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative per la sicurezza

La capacità di assicurare la sicurezza dei dati passa anche attraverso **specifiche tecniche**, come la crittografia e pseudonimizzazione.

L'accordo Stato-Regioni prevede espressamente **l'obbligo** di usare tecniche di **crittografia** per il trasferimento di dati, voce, video, immagini, documenti nell'ambito dei servizi di telemedicina.

Come vedremo nel prossimo capitolo, privacy e sicurezza dei dati vanno di pari passo.

Può esserci sicurezza senza privacy, ma non può esserci privacy senza sicurezza.

CYBERSECURITY E TELEMEDICINA

UNA QUESTIONE DI VITA O DI MORTE

LA SICUREZZA NON VIENE DOPO

L'obiettivo di qualsiasi buon medico è curare le persone e salvare vite. Per secoli la professione medica ha fatto uso di una moltitudine di **strumenti**, alcuni ormai cimeli da museo; altri ancora in uso oggi. Il mondo sta cambiando, ma il principio è sempre lo stesso: i medici hanno bisogno di strumenti all'avanguardia per curare le persone.

Oggi, questi strumenti sono servizi digitali, dispositivi, intelligenza artificiale e robot. La caratteristica comune? Sono tutti **connessi**, sempre.

Quando un dispositivo è connesso, è anche soggetto ad innumerevoli **minacce** che possono sfruttare le **vulnerabilità** presenti nell'hardware e software.

Cos'è la cybersecurity?

La cybersecurity è un insieme di discipline che si occupa di garantire la sicurezza dei sistemi connessi online. In realtà, oggi per cybersicurezza si intende generalmente il ben più ampio panorama della **sicurezza delle informazioni**.

Sicurezza delle informazioni (dati) non equivale a sicurezza dei sistemi ICT.

Non è sufficiente **investire in tecnologia** come software antivirus, firewall o server di ultima generazione per garantire la sicurezza delle informazioni.

I dati non sono mai statici, ma viaggiano continuamente attraverso flussi interni ed esterni che coinvolgono innumerevoli software, dispositivi, archivi, e diverse tipologie di soggetti.

La sicurezza dei dati si ottiene soltanto con un **approccio a 360 gradi**, che passa anche dall'innovazione tecnologica ma non si ferma lì.

Non è un problema dell'ufficio IT

La sicurezza dei dati e dei sistemi, in quanto linfa vitale della connected care, non può essere una preoccupazione dell'ufficio IT.

Il **top management** dovrebbe integrare la cybersecurity nelle proprie strategie di business, ascoltare i **responsabili della sicurezza** (in USA si chiamano Information security officers) e far sì che tutta la compagine aziendale sia allineata agli stessi obiettivi.

Strategia, analisi dei rischi, assunzione di responsabilità, gestione delle risorse. Sono solo alcune delle questioni che dovrebbero essere attivamente affrontate.

La cybersecurity non riguarda l'ufficio IT, e l'amministratore di sistema non è il responsabile della sicurezza delle informazioni.

L'accordo Stato-Regioni sulla telemedicina prevede la **designazione di un Direttore/Responsabile sanitario** che garantisce l'organizzazione tecnico-sanitaria e la sussistenza dei dovuti standard per le attività di telemedicina.
Questo significa che sarà il Direttore sanitario ad essere **responsabile della gestione della sicurezza** dei dati e del **rispetto della normativa privacy** per ogni attività di telemedicina.

La governance della cybersecurity

Come per la privacy, non può esserci sicurezza senza una concreta attività di **gestione della cybersecurity**.

La gestione della cybersecurity tocca quasi tutti gli ambiti aziendali, sovrapponendosi in alcuni casi anche con la normativa privacy.

Vediamone alcuni:

Business	Gestione del rischio fornitori
R&D	Security by design nel ciclo di sviluppo di prodotti e servizi
Architettura IT	Sicurezza delle reti, dispositivi, applicativi e business continuity
Legal & HR	Censimento dei flussi di dati, contrattualistica, compliance normativa, digital forensics

Anche in questo caso, **l'accordo Stato Regioni** sulla telemedicina impone agli operatori sanitari di adottare un **sistema di gestione** per la cybersecurity, comprensivo di un **piano di valutazione dei rischi** con rivalutazione periodica e adozione di misure di mitigazione.

In caso di violazioni di dati, dovute alla mancanza di un adeguato sistema di gestione, saranno applicabili le **disposizioni sanzionatorie** previste dal GDPR e (in caso di operatori essenziali) dalla Direttiva NIS.

Si può morire di virus informatico?

Ogni anno sempre più strutture sanitarie subiscono **attacchi ransomware**, che bloccano completamente i sistemi informatici. Nel mondo della connected care e della salute digitale, in cui talvolta neanche esiste una cartella clinica cartacea, è semplicemente inaccettabile.

Il 10 settembre 2020 un ospedale di Düsseldorf è stato infettato da un ransomware che ha bloccato tutti i sistemi informatici. Per diverso tempo l'ospedale non ha potuto accettare nuovi pazienti. Tra quelli rifiutati c'era una donna che è morta a causa dell'impossibilità di essere curata.

Qualcuno direbbe che **morire per colpa di un virus informatico** è follia, eppure sarà sempre più probabile.

Anche per questo motivo, l'accordo Stato Regioni sulla telemedicina prevede l'obbligo di identificare un soggetto responsabile per la manutenzione delle tecnologie per la telemedicina, così come l'obbligo di adottare **politiche per la sicurezza**, riservatezza, conservazione e integrità dei dati, conformemente alle normative italiane ed europee.

Chi ne risponde?

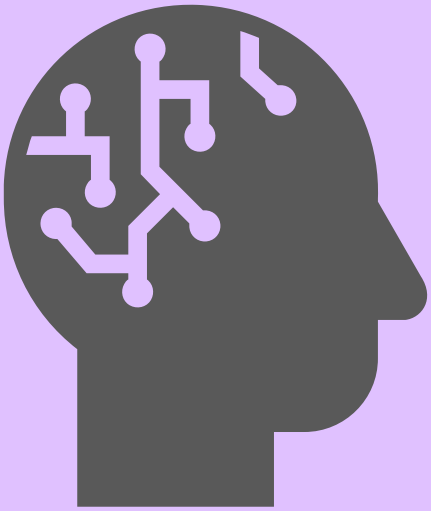
La legge 24/2017 (legge Gelli-Bianco) afferma che la **sicurezza delle cure** si realizza anche mediante l'insieme di tutte le attività finalizzate alla prevenzione e **gestione del rischio** connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative.

Secondo la normativa vigente, quindi, la struttura sanitaria è responsabile del **danno biologico** causato dal malfunzionamento o blocco dei sistemi informatici o dei dispositivi connessi (es. robot per la chirurgia), nel caso in cui non abbia adottato adeguate misure per la prevenzione e gestione del rischio.

Come già affermato, anche il recentissimo accordo Stato-Regioni prevede la responsabilità dell'operatore sanitario che non abbia adottato **servizi in grado di garantire la sicurezza** dei dati e il rispetto dei diritti dei pazienti (tra cui anche quelli previsti dal GDPR).

INTELLIGENZA ARTIFICIALE

LA NUOVA FRONTIERA DELLA MEDICINA



Cos'è l'intelligenza artificiale?

Per intelligenza artificiale ci si riferisce a sistemi che sono in grado di percepire l'ambiente, imparare autonomamente e prendere decisioni automatizzate.

In sostanza, sistemi che grazie all'acquisizione di dati su larga scala sono in grado di raggiungere gli obiettivi definiti dai programmatori, in modo autonomo e senza necessità di supervisione umana.

Quello che interessa particolarmente è il settore del **machine learning**, il campo di studi che dà ai software il potere di imparare dai dati acquisiti, evolvere e prendere decisioni senza bisogno di programmazione specifica.

Grazie al machine learning è oggi possibile automatizzare e rendere più efficienti moltissime attività umane. In alcuni casi, i risultati ottenuti dagli algoritmi di machine learning sono migliori rispetto a quelli ottenuti da una mente umana.

L'intelligenza artificiale non è soltanto machine learning. Ad esempio, anche il **natural language processing** è un importante campo dell'intelligenza artificiale, che dà vita ai **chatbot**.

L'intelligenza artificiale nella sanità digitale

Il dibattito sull'intelligenza artificiale nella sanità si concentra soprattutto su una **domanda** tanto semplice quanto fondamentale: i pazienti saranno più o meno tutelati?

Le macchine non si stancano di guardare radiografie, prendono decisioni in modo estremamente più veloce di un essere umano, ed imparano a riconoscere determinati pattern in minor tempo. Talvolta, sono in grado di riconoscere patterns impossibili da discernere da un essere umano.

Non bisogna però dimenticare che l'intelligenza artificiale è uno **strumento**, e come tale va governato. La tecnologia non è infallibile, e l'intelligenza artificiale soffre di **numerose problematiche**, esponendo i pazienti a rischi finora sconosciuti.

I principali rischi dell'intelligenza artificiale

Come menzionato, gli algoritmi di machine learning imparano analizzando enormi quantità di dati. Purtroppo, capita spesso che i dati usati in fase di training non siano sufficientemente rappresentativi, o che le modalità di apprendimento del software non siano appropriate per lo specifico contesto di utilizzo.

A questo deve aggiungersi l'effetto scatola nera degli algoritmi. I medici curanti (e spesso anche gli stessi sviluppatori) non sono in grado di capire quali sono le motivazioni che hanno portato ad una decisione automatizzata.

Bias nascosti	L'IA riproduce ed amplifica errori presenti nel dataset usato per il training.
Correlazioni errate	L'IA può trovare correlazioni dove non esistono, aumentando il rischio di diagnosi errate.
Scatola nera	I medici non hanno modo di comprendere davvero in che modo l'IA produce un risultato
Chatbots e 'self-help'	È inevitabile la diffusione di sistemi di 'self-help' a pagamento destinati ai consumatori, che potranno causare diseguaglianze e rischi di diagnosi errate.

Come mitigare i rischi?

L'intelligenza artificiale è una tecnologia rivoluzionaria che deve essere usata tenendo conto dei **rischi** che ne derivano.

Questi rischi devono essere gestiti attraverso adeguate **attività di auditing** durante il ciclo di sviluppo dell'algoritmo, che tengano conto di **privacy**, **sicurezza** ed **etica**.

Contemporaneamente, devono essere formati gli operatori ed i pazienti, informandoli dei rischi.

Infine, le aziende ospedaliere devono essere **responsabili della scelta** dei software di IA, tenendo conto delle garanzie offerte in relazione a privacy, sicurezza ed etica del trattamento.

Net Patrol Italia

www.netpatrol.it - info@netpatrol.it - 02 87165913

Sede di Milano
Via Napo Torriani, 31 | 20124 Milano

Sede di Udine
Via Giovanni Paolo II, 3 | 33100 Udine

GDPR INSIGHT SERIES, N° 6

SANITÀ DIGITALE

PRIVACY, CYBERSICUREZZA E INTELLIGENZA ARTIFICIALE NELLA SANITÀ DIGITALE

Novembre 2020