STEFANELLI & STEFANELLI STUDIO LEGALE

SANZIONI PRIVACY SETTORE SANITARIO

NELL'ANNO 2024



PREFAZIONE

Come ogni anno lo Studio Legale Stefanelli&Stefanelli continua a tenere monitorato l'andamento delle sanzioni del Garante Privacy nel settore della sanità.

Confrontando le sanzioni inflitte dall'Autorità nel 2024 con quelle comminate nel corso del 2023 emerge che:

- se nel 2023 destinatarie delle sanzioni erano per la maggior parte le pubbliche amministrazioni, nel 2024 soggetti **pubblici e privati** sono stati multati in egual misura
- tra questi ultimi continuano ad essere sanzionate in buona parte aziende fornitrici di **tecnologie sanitarie** e **cliniche private** ma si registra anche un aumento delle sanzioni a carico di **medici liberi professionisti**
- continua ad aumentare sia l'**importo totale delle sanzioni** comminate in sanità sia l'importo medio a carico dei singoli destinatari
- la risposta sanzionatoria dell'ammonimento è ancora più sporadica dell'anno precedente a fronte dell'88,6% di sanzioni pecuniarie;
- la maggior parte delle multe continua a derivare dalla **comunicazione illecita** di dati relativi alla salute o dall'accesso non autorizzato a tali dati. Tuttavia, è importante notare che nel 2024 molte di queste infrazioni sono state associate a un aumento delle sanzioni dovuto ad **attacchi informatici**.

PREFAZIONE

Quest'ultimo aspetto, in particolare, fa riflettere sulla necessità di gestire l'adeguamento al GDPR e alla normativa NIS2 in sinergia.

Le due norme, inatti, pur avendo obiettivi e ambiti di applicazione differenti, si completano e si sovrappongono nella protezione dei dati sanitari e nella sicurezza delle infrastrutture digitali.

Per questo motivo risulta essenziale adottare un approccio integrato per assicurare che le misure di cybersecurity rispettino le prescrizioni di entrambe le normative, evitando incoerenze o lacune, per frontreggiare l'emergenza rappresentata dall'aumento critico del crimine informatico in sanità.

Buona lettura!

Avv. Maria Livia Rizzo

INDICE DEI CONTENUTI

Strutture sanitarie pubbliche 6

OGGETTO DELLA SANZIONE

Accesso illecito ai dati 6

Accesso illecito ai dati + Rapporti con l'autorità Garante 11

Comunicazione di dati 12

Comunicazione di dati + Rapporti con l'autorità Garante 16

Perdita di dati + Rapporti con l'autorità Garante 17

Trattamento illecito dei dati + Violazione obblighi di trasparenza 18

Violazione del principio di esattezza + Richieste di esercizio di diritti 19

Strutture sanitarie private 20

OGGETTO DELLA SANZIONE

Violazione del principio di esattezza + Accesso illecito ai dati 20

Comunicazione di dati 21

Trattamento illecito dei dati 23

Medico libero professionista 24

OGGETTO DELLA SANZIONE

Comunicazione di dati 24

Richieste di esercizio di diritti + Rapporti con l'autorità Garante 26

Richieste di esercizio di diritti + Violazione obblighi di trasparenza 27

Trattamento illecito dei dati + Richieste di esercizio di diritti + Rapporti con l'autorità Garante 28

INDICE DEI CONTENUTI

Ente Pubblico 29

OGGETTO DELLA SANZIONE

Accesso illecito ai dati.....29

Imprese settore informatico.....31

OGGETTO DELLA SANZIONE

Accesso illecito ai dati.....31

Accesso illecito ai dati + Obblighi del responsabile + Rapporti con l'autorità Garante.....33

Violazione del principio di esattezza + Accesso illecito ai dati.....36

Imprese settore Medical Device.....37

OGGETTO DELLA SANZIONE

Comunicazione di dati + Violazione obblighi di trasparenza.....37

Centro Estetico 39

OGGETTO DELLA SANZIONE

Comunicazione di dati + Violazione obblighi di trasparenza + Trattamento illecito dei dati 39

Grafici riassuntivi.....41

Strutture sanitarie pubbliche

Accesso illecito ai dati

Accessi illeciti a DSE

	[doc. web n. 10001279]		
	Azienda Sanitaria dell'Alto Adige		
	22 Aprile 2024		Bolzano (BZ)
	€ 75.000		
Origine della sanzione	Reclamo		Notifica di Data Breach
Parametro impattato	**RISERVATEZZA**		
VIOLAZIONE 1	Ripetuti accessi al dossier da parte di personale sanitario che, sebbene autorizzato al trattamento, non era coinvolto nel processo di cura dei soggetti a cui i dossier sanitari si riferivano.		

Attacco informatico

	[doc. web n. 10074293]	
	Azienda Sanitaria Locale Città di Torino	
	4 Giugno 2024	Torino (TO)
	€ 8.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**DISPONIBILITÀ**	
VIOLAZIONE 1	Attacco informatico, determinato da un malware di tipo ransomware (HIVE), ai sistemi informativi dell'ASL che ha reso indisponibili i server ed i data store dell'azienda, ubicati nei 3 data center dei presidi ospedalieri. L'Azienda non aveva adottato adeguate misure per segmentare e segregare le reti su cui erano attestate le postazioni di lavoro dei propri dipendenti, nonché i sistemi (server) utilizzati per i trattamenti. Nello specifico, le VLAN non erano separate tra loro con apparati firewall. Inoltre, l'accesso remoto, tramite VPN, alla rete della ASL, avveniva mediante una procedura di autenticazione informatica basata solo sull'utilizzo di username e password; le credenziali di autenticazione utilizzate per l'accesso remoto alla rete e ai sistemi gestiti dalla azienda in VPN erano le stesse utilizzate per l'accesso ai sistemi di dominio (server e postazioni di lavoro); erano previste specifiche utenze amministrative per alcuni sistemi quali il server di posta elettronica, i firewall, le Storage Area Network (SAN) e non era prevista una differenziazione fra le utenze degli operatori con privilegi amministrativi e non.	

Attacco informatico

	[doc. web n. 10057610]	
	Azienda ULSS 6 Euganea	
	17 Luglio 2024	Padova (PD)
	€ 22.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA** **DISPONIBILITÀ**	
VIOLAZIONE 1	Attacco informatico che ha precluso l'accesso e la disponibilità ad alcuni applicativi aziendali (infrastrutturali, ospedalieri, amministrativi, territoriali) tramite un ransomware che ha crittografato macchine virtuali, aggiungendo l'estensione "lockbit" ai nomi dei file. Gli attaccanti hanno avuto accesso ai sistemi VmWare, utilizzando l'utente "root" per sospendere le macchine virtuali ed eseguire la cifratura dei datastore. L'attacco ha interessato la console di virtualizzazione degli applicativi sanitari e parte delle postazioni di lavoro. È stata identificata una potenziale esfiltrazione di circa 17.000 documenti contenenti dati personali e non. È stato rilevato un trasferimento dati di circa 700 MB da 18 client. I dati pubblicati non sono stati esfiltrati dai database, ma provenivano dalle postazioni di lavoro dei dipendenti che avevano salvato localmente documenti personali, liste di lavoro (es. ricoveri, dimissioni) o schede di pazienti, talvolta in bozza o incomplete e non catalogate, contravvenendo alle istruzioni aziendali che prevedevano l'uso esclusivo di cartelle condivise o sistemi dedicati. Il perimetro della violazione è stato delimitato a 9.520 interessati e 5.763 file coinvolti.	

Attacco informatico

	[doc. web n. 10086523]	
	Azienda Ospedaliero-Universitaria SS. Antonio e Biagio e Cesare Arrigo	
	17 Ottobre 2024	Alessandria (AL)
	€ 25.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA** **DISPONIBILITÀ**	
VIOLAZIONE 1	Attacco informatico ai sistemi informativi dell'Azienda determinato da un malware di tipo ransomware "Ragnar Locker". Il punto di origine, sebbene non vi fossero evidenze certe per la mancanza di un sistema di log management aziendale, sembra essere stato lo sfruttamento di una vulnerabilità del firewall aziendale. Attraverso tale vulnerabilità, gli attaccanti hanno recuperato credenziali di dominio e condotto movimenti laterali mediante una connessione VPN any to any, che ha consentito l'accesso a un PC aziendale con VPN aperta. Al momento della violazione, le utenze di "manutenzione" erano spesso generiche, non individuali, con massimi privilegi amministrativi, e non era prevista una procedura di autenticazione a più fattori (MFA) per l'accesso remoto in VPN. Gli attaccanti Hanno effettuato una privilege escalation ad amministratore, scaricato le credenziali memorizzate nel servizio LSASS e, infine, eseguito il download massivo dei contenuti del file server su uno storage situato in Olanda, oltre all'installazione di una backdoor SSH. Non erano adottate misure di sicurezza per proteggere e limitare l'accesso all'area di memoria utilizzata dal processo lsass. exe. Gli attaccanti hanno disattivato l'antivirus e inoculato il codice eseguibile che ha scaricato la ransom note sulle postazioni di lavoro, sebbene non abbiano proceduto alla cifratura dei dati. L'attacco ha riguardato le postazioni di lavoro (PdL) e il sistema di file sharing, che di fatto era utilizzato come unico gestore documentale. Le cartelle del file server erano accessibili da qualsiasi postazione di lavoro dell'ospedale. Le categorie di dati impattati includono dati anagrafici (nome, cognome, sesso, data e luogo di nascita, codice fiscale), dati di contatto (indirizzo postale/elettronico, numero di telefono), dati di accesso e identificazione (username, password) e dati relativi alla salute per utenti, fornitori e pazienti, nonché dipendenti. Per i dipendenti, i dati riguardavano documentazione normo-economica ed eventuali contenuti personali depositati nelle cartelle del file server.	

Attacco informatico

	[doc. web n. 10104860]	
	Azienda Socio Sanitaria Territoriale Fatebenefratelli-Sacco	
	14 Novembre 2024	Milano (MI)
	€ 40.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA** **DISPONIBILITÀ**	
VIOLAZIONE 1	Attacco informatico, condotto dal gruppo denominato Vice Society, determinato da un malware di tipo ransomware che ha causato il malfunzionamento degli applicativi informatici e l'esfiltrazione di dati che ha coinvolto un'area di un file server a disposizione degli utenti aziendali che accedono per mezzo di cartelle condivise.	

Accesso illicito ai dati

Rapporti con l'autorità Garante

Attacco informatico;
Notifica di data breach tardiva;
Registro delle violazioni non conforme

	[doc. web n. 10002533]	
	ASL Roma 3	
	21 Marzo 2024	Roma
	€ 10.000	
Origine della sanzione	Notifica di Data Breach di altri titolari	Notizie di stampa
Parametro impattato	**DISPONIBILITÀ**	
VIOLAZIONE 1	L'Azienda non ha provveduto a notificare la violazione dei dati personali all'Autorità Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, in relazione a un attacco informatico di tipo ransomware che ha colpito i sistemi gestiti da LAZIOcrea S.p.a. e ha reso indisponibili dati sanitari	
VIOLAZIONE 2	L'Azienda non ha provveduto a documentare adeguatamente la violazione dei dati personali, comprese le circostanze relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio	

Comunicazione di dati

Trasmissione di dati relativi alla salute a soggetto non autorizzato

	[doc. web n. 9997395]	
	Azienda sanitaria locale Vercelli - Ospedale Sant'Andrea	
	22 Febbraio 2024	Vercelli (VC)
	Ammonimento	
Origine della sanzione	Segnalazione	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Consegna a una paziente di cartella clinica contenente gli esami medici anche relativi ad un'altra persona, a causa della applicazione accidentale di un'etichetta nominativa di reparto, recante il nome di una paziente su un tracciato cardiotocografico effettuato da un'altra paziente.	

Invio di e-mail con destinatari visibili

	[doc. web n. 10037439]	
	Azienda Sanitaria Locale TO4	
	23 Maggio 2024	Chivasso (TO)
	€ 8.400	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Trasmissione da parte dell'addetto della segreteria dell'ambulatorio di neurologia, per errore umano, di una email contenente una circolare di istruzioni sul piano terapeutico (privo di indicazioni specifiche) a n. 45 indirizzi di pazienti affetti da sclerosi multipla, inserendo i relativi indirizzi in campo CC in chiaro e, dopo circa mezz'ora, una seconda email di rettifica della prima con le medesime modalità.	

Trasmissione di dati relativi alla salute a soggetto non autorizzato

	[doc. web n. 10079346]	
	Azienda Sanitaria Territoriale di Ascoli Piceno	
	26 Settembre 2024	Ascoli Piceno (AP)
	€ 17.000	
Origine della sanzione	Reclamo	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Rilascio di certificazioni (da presentare al datore di lavoro come giustificazione dell'assenza) attestanti la presenza in ospedale della lavoratrice reclamante che riportavano l'indicazione del reparto che aveva erogato la prestazione sanitaria e il timbro con la specializzazione del medico (neurologia, ginecologia, ortopedia), da cui potevano desumersi informazioni sullo stato di salute.	

Trasmissione di dati relativi alla salute a soggetto non autorizzato

	[doc. web n. 10039453]	
	AUSL della Romagna	
	6 Giugno 2024	Ravenna (RA)
	€ 24.000	
Origine della sanzione	Reclamo	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Trasmissione di dati personali della reclamante relativi all'infezione da HIV al Dipartimento dell'amministrazione penitenziaria-Direzione casa circondariale di Rimini. La reclamante, rispetto alla quale era stata accertata una invalidità nella misura del 75%, era assistita dal genero, il quale aveva richiesto all'Amministrazione Penitenziaria del Ministero della Giustizia-Casa circondariale di Rimini, presso la quale prestava servizio, i benefici previsti dalla legge 5 febbraio 1992, n. 104. L'Amministrazione Penitenziaria, nell'intento di procedere ad accertamenti a campione riguardo l'autenticità dei verbali di accertamento dello stato di persona con handicap grave ai sensi dell'art. 3, comma 3, della citata legge n. 104/1992 prodotti da personale dipendente che fruiva dei benefici previsti dalla predetta norma, chiedeva all'Azienda, di confermare o meno l'esistenza agli atti di un verbale di accertamento dello stato di handicap relativo alla persona della reclamante. A seguito di tale richiesta, l'Azienda forniva riscontro trasmettendo «copia del verbale di L 104/92 presente nel fascicolo AUSL della XX». La copia del verbale inoltrato con la predetta comunicazione era costituita dalla riproduzione fotografica integrale del verbale della Commissione Medica "in chiaro", totalmente leggibile e senza alcun tipo di mascheramento, con l'anamnesi completa e la valutazione dell'handicap. Da tale verbale, inoltrato all'amministrazione carceraria in versione completa e integralmente leggibile, emerge inequivocabilmente che tra le patologie patite dalla reclamante risulta anche l'infezione HIV e la nefropatia HIV relata.	

Trasmissione di dati relativi alla salute a soggetto non autorizzato

	[doc. web n. 10102444]	
	Azienda Sanitaria dell'Alto Adige	
	12 Dicembre 2024	Bolzano (BZ)
	€ 5.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE 1	Un medico convenzionato che opera presso gli ambulatori dell'Azienda sanitaria, relativamente alla tematica "riduzione orario di servizio", ha scritto a diversi soggetti aziendali ed esterni (info@ordinemedici.bz.it) allegando alla sua comunicazione la lista dei pazienti visitati in un determinato giorno. La comunicazione è stata inviata in chiaro e nella stessa erano riportati i seguenti dati: nome – cognome – data di nascita – residenza del paziente nonché sede di erogazione prestazione, prestazione erogata, indicazione su paziente pagante, esente (con indicazione del codice di esenzione), CF e numero di cellulare.	

Comunicazione di dati

Rapporti con l'autorità Garante

Trasmissione di dati relativi alla salute a soggetto non autorizzato;
Mancato riscontro a richiesta di informazioni del Garante

	[doc. web n. 9994882]
	Azienda socio-sanitaria locale n. 1 di Sassari
8 Febbraio 2024	Sassari (SS)
	€ 18.000
Origine della sanzione	Reclamo
Parametro impattato	**RISERVATEZZA**
VIOLAZIONE 1	Trasmissione, da parte dell'Azienda socio-sanitaria locale n. 1 di Sassari di una mail rivolta alla reclamante, ma ad un indirizzo e-mail non appartenente alla stessa. In particolare, la mail conteneva il provvedimento con il quale l'Ufficio ricoveri Extra-Regione, Distretto di Sassari dell'Azienda, negava la concessione di benefici economici, quali spese di viaggio e soggiorno, per usufruire di prestazioni sanitarie ai sensi della L. R. n. 26/1991 presso una struttura sanitaria privata extra-regione. Secondo quanto dichiarato e documentato dalla reclamante, il documento conteneva i dati identificativi della stessa, l'indicazione dell'Azienda Ospedaliera presso la quale avrebbe inteso ricevere le cure sanitarie nonché alcune elementi relativi al percorso medico intrapreso e da intraprendere.
VIOLAZIONE 2	Mancato riscontro alla richiesta di informazioni da parte del Garante (condotta omissiva illecita in violazione dell'art. 157 - richiesta di informazioni e di esibizione di documenti - in relazione all'art. 166, comma 2, del Codice.)

Perdita di dati

Rapporti con l'autorità Garante

Perdita di documentazione sanitaria; Mancata notifica di data breach al Garante

	[doc. web n. 10107405]	
	Azienda Sanitaria Provinciale di Enna- Distretto sanitario di Nicosia	
	19 Dicembre 2024	Enna (EN)
	€ 8.000	
Origine della sanzione	Reclamo	
Parametro impattato	**DISPONIBILITÀ**	
VIOLAZIONE 1	A seguito di richiesta reiterata di accesso agli atti avanzata all'Azienda sanitaria per il rilascio del verbale redatto dalla Commissione per malati gravissimi cui era stata sottoposta la sorella, di cui la reclamante è amministratore di sostegno, l'Azienda sanitaria comunicava che il documento richiesto e predisposto per il rilascio non è più rinvenibile agli atti dell'ufficio.	
VIOLAZIONE 2	Mancata notifica di violazione dei dati personali all'Autorità di controllo	

Trattamento illecito dei dati

Violazione obblighi di trasparenza

Assenza di DPIA;
Informativa privacy non conforme;
Consenso non conforme

	[doc. web n. 10057629]	
	Istituto Tumori Giovanni Paolo II di Bari	
	17 Luglio 2024	Bari (BA)
	€ 10.000	
Origine della sanzione	Attività Ispettiva	
Parametro impattato	**CORRETTEZZA ADEMPIMENTI**	
VIOLAZIONE 1	Mancato adempimento dell'obbligo di svolgere e pubblicare la Vip in relazione alla raccolta e al successivo trattamento dei dati dei pazienti deceduti e non contattabili in violazione degli artt. 110 prima parte del comma 1 e 110-bis, comma 4 del Codice.	
VIOLAZIONE 2	Svolgimento della valutazione d'impatto circoscritto ad un numero di casi di gran lunga inferiore a quelli per i quali esso, quand'anche non richiesto dalla legge ai sensi del combinato disposto degli artt. 110 e 110-bis comma 4 del Codice, sia comunque necessario ai sensi dell'art. 35 del Regolamento (trattamento di dati sulla salute - e se del caso anche quelli genetici, quelli idonei a rilevare l'origine razziale ed etnica, o relativi alla vita e all'orientamento sessuale - riferiti a soggetti vulnerabili, quali sono i pazienti e/o i minori).	
VIOLAZIONE 3	Raccolta inidonea di due differenti consensi (il primo acquisito in occasione delle prestazioni sanitarie e volto ad autorizzare il trattamento dei dati per scopi di ricerca medica in determinati settori, salva la possibilità di acquisire un consenso ulteriore rispetto a specifici progetti) in quanto il settore della ricerca scientifica da indicarsi nel modulo di consenso si limita a individuare macro finalità della ricerca stessa e non uno specifico progetto.	
VIOLAZIONE 4	Assenza di una informativa privacy completa dei suoi elementi essenziali	

Violazione del principio di esattezza

Richieste di esercizio di diritti

Mancato riscontro a richiesta di esercizio dei diritti; Tardiva rettifica dei dati inesatti

	[doc. web n. 10036837]	
	Azienda socio-sanitaria territoriale Rhodense	
	23 Maggio 2024	Garbagnate (MI)
	€ 4.500	
Origine della sanzione	Reclamo	
Parametro impattato	**INTEGRITÀ**	
VIOLAZIONE 1	Mancato riscontro a richiesta di rettifica dei dati personali del reclamante (nello specifico, gli indirizzi fisici di residenza anagrafica e di domicilio sanitario) erroneamente registrati nel sistema informativo sanitario regionale, così come palesemente appariva sia dalla consultazione del Fascicolo Sanitario Elettronico dell'interessato, sia dai dati riportati sulle ricette elettroniche redatte dal medico di assistenza primaria.	

Strutture sanitarie private



Violazione del principio di esattezza



Accesso illecito ai dati

Errori nella attribuzione di prestazioni sanitarie

	[doc. web n. 9988652]	
	Ospedale Pediatrico Bambino Gesù	
	24 Gennaio 2024	Roma
	€ 8.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**INTEGRITÀ** **RISERVATEZZA**	
VIOLAZIONE	Accesso da parte di alcuni pazienti (tramite il portale dedicato "Carta della Salute" https://cartadellasalute.ospedalebambinogesu.it) a refertio di altra pazienti a causa dell'invio, da parte del sistema del fornitore Dedalus Italia S.p.A., al sistema di gestione dati dell'Ospedale (middleware Mirth) di messaggi HL7 di laboratorio contenenti un segmento di informazione riportante un identificativo paziente diverso rispetto al contenuto del messaggio (referto). La propagazione successiva di questi messaggi ha generato un'associazione errata tra referto e paziente negli altri applicativi integrati. L'effetto della suddetta anomalia è stata l'associazione di un referto, integro e coerente nel suo insieme, ad un paziente sbagliato.	

Comunicazione di dati

Trasmissione di dati relativi alla salute a soggetto non autorizzato

	[doc. web n. 10057346]	
	Clinica - nome non presente nel provvedimento	
	[doc. web n. 10057329]	
	Associazione - nome non presente nel provvedimento	
	17 Luglio 2024	Non indicato
	Ammonimento	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	L'Ostetrica operante presso la clinica XX - per l'Associazione XX - inviava ad una paziente mail con allegato il modulo denominato "Consenso informato PMA fecondazione in vitro", affinché la signora e il compagno provvedessero alla compilazione dello stesso, al fine di fornire il consenso informato a specifico trattamento sanitario, come previsto da normativa. Per errore materiale, il modulo allegato conteneva già i dati di un'altra coppia di pazienti. L'Associazione agisce — per il tramite dei propri associati, soggetti autorizzati al trattamento - in qualità di Responsabile esterno del Trattamento per la società XX, relativamente all'esercizio delle attività di ostetricia e ginecologia, in particolare per l'accertamento, la cura e la terapia delle problematiche relative o connesse alla sterilità di coppia.	

Trasmissione di dati relativi alla salute a soggetto non autorizzato

	[doc. web n. 10074551]	
	Società di servizi sanitari polispecialistici - Bios s.p.a.	
	17 Ottobre 2024	Roma
	€ 7.000	
Origine della sanzione	Reclamo	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	La società, inserendo un indirizzo di posta errato, ha diffuso il referto di esami diagnostici relativi alla figlia minore della reclamante, che conteneva oltre ai dati sanitari della minore, anche tutti i dati anagrafici della stessa (luogo, data di nascita, residenza. elnoltre, i referti erano meramente allegati all'e-mail senza richiedere per la loro visione una password di accesso.	

Trattamento illecito dei dati

Base giuridica mancante; Informativa privacy mancante

	[doc. web n. 10109794]	
	Poliambulatorio - Centro Medico Green Life S.r.l	
	19 Dicembre 2024	Conegliano (TV)
	€ 5.000	
Origine della sanzione	Attività Ispettiva	
Parametro impattato	**CORRETTEZZA ADEMPIMENTI**	
VIOLAZIONE	Impianto di videosorveglianza, costituito da quattro telecamere esterne e una interna, non segnalato da cartelli informativi e senza previa richiesta di autorizzazione all'Ispettorato del Lavoro, a fronte della presenza di un lavoratore dipendente.	

Medico libero professionista

Comunicazione di dati

Diffusione di dati relativi alla salute

	[doc. web n. 9983244]		
	Medico specialista - Dott. Bagnato		
	11 Gennaio 2024		Non indicato
	€ 20.000		
Origine della sanzione	Segnalazione		
Parametro impattato	**RISERVATEZZA**		
VIOLAZIONE	Sul muro esterno dello Studio medico, a lato della porta di ingresso dello studio e nelle sue immediate vicinanze erano affissi una cassetta delle poste e un contenitore di metallo, entrambi privi di qualsiasi nominativo. Sul contenitore, tuttavia, era riportata l'indicazione "solo ricette mediche" mentre nella serratura del contenitore era inserita una chiave. Detto contenitore, inoltre, era a libero accesso del pubblico in quanto, nel corso del servizio, sono state viste diverse persone che lo hanno aperto ed hanno prelevato dei foglietti di carta che si trovavano al suo interno. All'interno del contenitore "erano conservate numerose prescrizioni mediche, gran parte delle quali costituite da "ricetta elettronica — promemoria per l'assistito" e, per la restante, da "ricette rosa" tratte da ricettario del SSN. Le ricette erano state compilate a favore di diversi nominativi, alcune riportavano la firma del medico (nel caso delle ricette del SSN) e tutte erano accessibili a chiunque atteso che le stesse (ad eccezione di un caso) non erano neppure riposte all'interno di buste chiuse; nel contenitore erano riposte n. 67 ricette. Da un esame estemporaneo delle stesse era possibile rilevare che le prescrizioni mediche erano state emesse a favore di soggetti diversi e riportavano prescrizioni sia di medicinali che di esami specialistici.		

Trasmissione di dati relativi alla salute a soggetto non autorizzato

	[doc. web n. 10064128]	
	Medico specialista - Nominativo non indicato	
	12 Settembre 2024	 Non indicato
	Ammonimento	
Origine della sanzione	 Reclamo	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Rilascio da parte del MMG di documentazione sanitaria, in busta chiusa, al marito dell'interessata in assenza di delega scritta, a seguito di richiesta da parte della reclamante della consegna dello storico clinico e di tutta la documentazione clinica riferita al padre deceduto.	

Diffusione di dati relativi alla salute

	[doc. web n. 10095836]	
	Medico specialista - Dott. Rubino	
	12 Dicembre 2024	 Non indicato
	€ 20.000	
Origine della sanzione	 Reclamo	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Diffusione sul social media Instagram di fotografie nelle quali la reclamante è ripresa durante un intervento di medicina estetica.	

Richieste di esercizio di diritti

Rapporti con l'autorità Garante

Mancato riscontro a richiesta di esercizio dei diritti; Mancato riscontro a richiesta di informazioni del Garante

	[doc. web n. 10070330]	
	Medico specialista - Dott. De Vita	
	17 Luglio 2024	Non indicato
	€ 4.000	
Origine della sanzione	Reclamo	
Parametro impattato	**CORRETTEZZA ADEMPIMENTI**	
VIOLAZIONE 1	Mancato riscontro a richiesta di copia conforme di tutte le fotografie effettuate sulla persona della reclamante prima e dopo l'intervento chirurgico di rinosettoplastica.	
VIOLAZIONE 2	Mancato riscontro alla richiesta di informazioni da parte del Garante (condotta omissiva illecita in violazione dell'art. 157 - richiesta di informazioni e di esibizione di documenti - in relazione all'art. 166, comma 2, del Codice.)	

Richieste di esercizio di diritti

Violazione obblighi di trasparenza

Mancato riscontro a richiesta di esercizio dei diritti; Informativa privacy non conforme

	[doc. web n. 10037411]	
	Medico specialista - Nominativo non indicato	
	20 Giugno 2024	Non indicato
	€ 4.000	
Origine della sanzione	Reclamo	
Parametro impattato	**CORRETTEZZA ADEMPIMENTI**	
VIOLAZIONE 1	Mancato riscontro da parte del medico a una richiesta di accesso ai propri dati personali da parte della reclamante che richiedeva di accedere alle fotografie preoperatorie relative a un intervento effettuato dal professionista	
VIOLAZIONE 2	Insufficiente indicazione nell'informativa privacy del periodo di conservazione dei dati da fornire agli interessati	

Trattamento illecito dei dati

Richieste di esercizio di diritti

Rapporti con l'autorità Garante

Informativa privacy mancante; Mancato riscontro a richiesta di esercizio dei diritti; Mancato riscontro a richiesta di informazioni del Garante

	[doc. web n. 10072669]	
	Medico specialista - Dott. Francini	
	17 Ottobre 2024	Non indicato
	€ 6.500	
Origine della sanzione	Reclamo	
Parametro impattato	**CORRETTEZZA ADEMPIMENTI**	
VIOLAZIONE 1	Assenza di informativa privacy in relazione alla registrazione delle sedute di psicoterapia effettuate con strumenti audio.	
VIOLAZIONE 2	Mancato riscontro all'istanza con la quale il reclamante aveva chiesto "(...) quali dati erano in possesso (...) (del dott. Francini)", nonché "copia delle registrazioni, la documentazione privacy sottoscritta e/o presente presso (...) lo studio (informativa ai sensi dell'art. 13 del Regolamento) (e) le modalità di conservazione delle registrazioni e/o eventuale divulgazione delle medesime".	
VIOLAZIONE 3	Mancato riscontro alla richiesta di informazioni da parte del Garante (condotta omissiva illecita in violazione dell'art. 157 - richiesta di informazioni e di esibizione di documenti - in relazione all'art. 166, comma 2, del Codice.)	

Ente Pubblico

Accesso illecito ai dati

Attacco informatico

	[doc. web n. 10008177]	
	Ministero della Salute	
	7 Marzo 2024	Roma
	€ 100.000	
Origine della sanzione	Notizie Stampa	
	Comunicazione informale del Ministero	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Accessi non autorizzatiai sistemi riferiti alla piattaforma del Nuovo Sistema Informativo Sanitario (NSIS) a seguito dell'acquisizione illecita di 1.578 credenziali di autenticazione a seguito di attacco informatico" di cui il Ministero apprendeva notizia mediante una e-mail da parte di un utente che segnalava di aver individuato informazioni afferenti l'Amministrazione in un annuncio presente sul darkweb.	

Attacco informatico

	[doc. web n. 10002287]		
	Regione Lazio		
	21 Marzo 2024		Roma
	€ 120.000		
Origine della sanzione	Notifica di Data Breach		
Parametro impattato	**DISPONIBILITÀ**		
VIOLAZIONE	Attacco informatico, determinato da un malware di tipo ransomware, ai sistemi informativi gestiti da LAZIOcrea S.p.a. in qualità di responsabile del trattamento per conto della Regione e di diversi enti del servizio sanitario regionale. I sistemi colpiti trattavano dati sulla salute degli assistiti del Servizio sanitario regionale. L'attacco è stato originato dalla compromissione di un account appartenente a un dipendente regionale le cui credenziali di accesso sono state sottratte tramite artefatti malevoli (backdoor). Questi software malevoli sono stati inoculati su un computer client che operava da remoto tramite VPN, creando un canale di comunicazione tra il computer infetto e il gruppo di cybercriminali (al momento della violazione non era prevista una procedura di autenticazione informatica a più fattori per l'accesso VPN). Le credenziali di autenticazione sottratte sono state utilizzate per accedere da remoto alla rete della Società e condurre azioni prodromiche all'attacco. I cybercriminali hanno effettuato attività di scansione per acquisire informazioni sulla rete e sui sistemi server presenti. Sfruttando le credenziali compromesse, sono riusciti a muoversi "lateralmente" all'interno delle sotto-reti. Durante le attività di scansione, gli aggressori hanno individuato il server con hostname "RLWSIRIFT01", su cui era installato software di base obsoleto (Windows Server 2008 R2 Standard) per cui non erano più disponibili aggiornamenti o patch di sicurezza del produttore. Sfruttando vulnerabilità note del software obsoleto su questo server, i malintenzionati sono riusciti a ottenere credenziali di autenticazione con privilegi amministrativi, utilizzate nelle fasi successive dell'attacco. La conseguenza principale dell'attacco è stata la temporanea indisponibilità di numerosi sistemi informativi, che ha riguardato circa 180 sistemi server virtuali, rendendo i dati in essi trattati inaccessibili.		

Imprese settore informatico

Accesso illecito ai dati

Diffusione di dati relativi alla salute

	[doc. web n. 10095761]	
	Molise dati S.p.A	
	27 Novembre 2024	Campobasso (CB)
	€ 10.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Il Portale regionale del FSE (https://fse.regione.molise.it) a causa di una vulnerabilità del sistema aveva consentito a un soggetto terzo attraverso una manipolazione intenzionale della URL di effettuare una ricerca dei dati di altri cittadini presenti in Anagrafe Regionale del Molise. Nello specifico, manipolando la URL da https://fse.regione.molise.it/fseui/dashboard in https://fse.regione.molise.it/fseui/list l'utente è stato in grado di utilizzare la funzionalità di ricerca cittadino e successivamente selezionandolo accedere alla funzionalità di consultazione dei dati anagrafici e di consultazione del FSE del cittadino stesso. Il numero di assistiti coinvolti è stato pari a 7. A valle dell'analisi dei requisiti tecnici e funzionali del FSE alla quale hanno partecipato Regione Molise, Molise Dati, Tim S.p.A. ed Engineering S.p.A., il sistema è stato progettato e realizzato dal punto di vista informatico da Engineering S.p.A, che, pertanto, rappresenta il soggetto responsabile della progettazione delle procedure di identificazione e autenticazione informatica (Identity Management) nonché di autorizzazione informatica degli assistiti ai fini della consultazione dei documenti presenti nel FSE e delle misure a garanzia della riservatezza dei medesimi documenti.	

Diffusione di dati relativi alla salute

	[doc. web n. 10095810]	
	Engineering ingegneria informatica S.p.A.	
	27 Novembre 2024	Roma
	€ 10.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE	Il Portale regionale del FSE (https://fse.regione.molise.it) a causa di una vulnerabilità del sistema aveva consentito a un soggetto terzo attraverso una manipolazione intenzionale della URL di effettuare una ricerca dei dati di altri cittadini presenti in Anagrafe Regionale del Molise. Nello specifico, manipolando la URL da https://fse.regione.molise.it/fseui/dashboard in https://fse.regione.molise.it/fseui/list l'utente è stato in grado di utilizzare la funzionalità di ricerca cittadino e successivamente selezionandolo accedere alla funzionalità di consultazione dei dati anagrafici e di consultazione del FSE del cittadino stesso. Il numero di assistiti coinvolti è stato pari a 7. A valle dell'analisi dei requisiti tecnici e funzionali del FSE alla quale hanno partecipato Regione Molise, Molise Dati, Tim S.p.A. ed Engineering S.p.A., il sistema è stato progettato e realizzato dal punto di vista informatico da Engineering S.p.A, che, pertanto, rappresenta il soggetto responsabile della progettazione delle procedure di identificazione e autenticazione informatica (Identity Management) nonché di autorizzazione informatica degli assistiti ai fini della consultazione dei documenti presenti nel FSE e delle misure a garanzia della riservatezza dei medesimi documenti.	

Accesso illecito ai dati

Obblighi del responsabile

Rapporti con l'autorità Garante

Attacco informatico;
Tardivo avviso di data breach al titolare;
Notifica di data breach tardiva;
Registro delle violazioni non conforme

	[doc. web n. 10002324]	
	LAZIOcrea S.p.a.	
	21 Marzo 2024	Roma
	€ 271.000	
Origine della sanzione	Notifica di Data Breach	
	Notizie Stampa	
Parametro impattato	**RISERVATEZZA** **INTEGRITÀ**	

VIOLAZIONE 1	Attacco informatico, determinato da un malware di tipo ransomware, ai sistemi informativi gestiti da LAZIOcrea S.p.a. in qualità di responsabile del trattamento per conto della Regione e di diversi enti del servizio sanitario regionale. I sistemi colpiti trattavano dati sulla salute degli assistiti del Servizio sanitario regionale. L'attacco è stato originato dalla compromissione di un account appartenente a un dipendente regionale le cui credenziali di accesso sono state sottratte tramite artefatti malevoli (backdoor). Questi software malevoli sono stati inoculati su un computer client che operava da remoto tramite VPN, creando un canale di comunicazione tra il computer infetto e il gruppo di cybercriminali (al momento della violazione non era prevista una procedura di autenticazione informatica a più fattori per l'accesso VPN). Le credenziali di autenticazione sottratte sono state utilizzate per accedere da remoto alla rete della Società e condurre azioni prodromiche all'attacco. I cybercriminali hanno effettuato attività di scansione per acquisire informazioni sulla rete e sui sistemi server presenti. Sfruttando le credenziali compromesse, sono riusciti a muoversi "lateralmente" all'interno delle sotto-reti. Durante le attività di scansione, gli aggressori hanno individuato il server con hostname "RLWSIRIFT01", su cui era installato software di base obsoleto (Windows Server 2008 R2 Standard) per cui non erano più disponibili aggiornamenti o patch di sicurezza del produttore. Sfruttando vulnerabilità note del software obsoleto su questo server, i malintenzionati sono riusciti a ottenere credenziali di autenticazione con privilegi amministrativi, utilizzate nelle fasi successive dell'attacco. La conseguenza principale dell'attacco è stata la temporanea indisponibilità di numerosi sistemi informativi, che ha riguardato circa 180 sistemi server virtuali, rendendo i dati in essi trattati inaccessibili.
VIOLAZIONE 2	LAZIOcrea, in qualità di responsabile del trattamento, ha informato tardivamente la Regione Lazio e gli altri titolari del trattamento coinvolti (circa due settimane dopo essere venuta a conoscenza dell'incidente).
VIOLAZIONE 3	LAZIOcrea ha violato l'obbligo di notificare la violazione dei dati personali senza ingiustificato ritardo, e comunque entro 72 ore dal momento in cui ne è venuta a conoscenza. La Società è venuta a conoscenza della violazione il 1° agosto 2021 ma l'ha notificata solo in data successiva, giustificando il ritardo con la necessità di acquisire gli elementi minimi, ripristinare i servizi essenziali e accertare la portata dell'incidente. Il Garante ha ritenuto tali motivazioni insufficienti, evidenziando che la notifica avrebbe dovuto avvenire per fasi, fornendo le informazioni disponibili

VIOLAZIONE 4	La Società non ha documentato adeguatamente la violazione. Il registro degli incidenti di sicurezza tenuto dalla Società non conteneva tutte le informazioni previste (come data e ora di chiusura e risoluzione, soggetto che ha rilevato l'incidente, altre organizzazioni contattate) e alcune delle informazioni presenti erano inesatte o poco dettagliate. Mancavano anche informazioni chiave come gli effetti e le conseguenze per gli interessati, la valutazione del rischio e le giustificazioni per il ritardo nella notifica

Violazione del principio di esattezza

Accesso illecito ai dati

Errori nella attribuzione di prestazioni sanitarie

	[doc. web n. 9990640]	
	Dedalus Italia S.p.a.	
	24 Gennaio 2024	Firenze (FI)
	€ 8.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA** **INTEGRITÀ**	
VIOLAZIONE	Accesso da parte di alcuni pazienti (tramite il portale dedicato "Carta della Salute" https://cartadellasalute.ospedalebambinogesu.it) a refertio di altra pazienti a causa dell'invio, da parte del sistema del fornitore Dedalus Italia S.p.A., al sistema di gestione dati dell'Ospedale (middleware Mirth) di messaggi HL7 di laboratorio contenenti un segmento di informazione riportante un identificativo paziente diverso rispetto al contenuto del messaggio (referto). La propagazione successiva di questi messaggi ha generato un'associazione errata tra referto e paziente negli altri applicativi integrati. L'effetto della suddetta anomalia è stata l'associazione di un referto, integro e coerente nel suo insieme, ad un paziente sbagliato.	

Imprese settore Medical Device

Comunicazione di dati

Violazione obblighi di trasparenza

Invio di e-mail con destinatari visibili; Informativa privacy non conforme

	[doc. web n. 9991183]	
	Medtronic Italia S.p.a.	
	8 Febbraio 2024	Milano (MI)
	€ 1300.000	
Origine della sanzione	Notifica di Data Breach	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE 1	Un membro del team Medtronic Diabete ha inviato una notifica via e-mail agli utenti dell'app MiniMed Mobile situati in vari paesi all'interno e all'esterno dell'UE per informarli su (1) un aggiornamento di manutenzione del server e (2) l'obbligo per gli utenti di accedere nuovamente al software CareLinkTM Personal, come parte di questo aggiornamento di manutenzione del server. Sono state inviate un totale di 11 notifiche e-mail, utilizzando Microsoft Outlook, come soluzione temporanea in attesa dell'implementazione di un nuovo processo automatizzato. 10 notifiche e-mail contenevano tra 490 e 495 indirizzi e-mail, mentre 1 notifica e-mail conteneva 8 indirizzi e-mail. Il membro del team Diabete ha incluso gli indirizzi e-mail dei destinatari nel campo "A", anziché nel campo "CCN". A causa di questo errore umano, gli indirizzi e-mail dei destinatari erano visibili agli altri destinatari, ovvero circa 489-494 destinatari o 7 destinatari, a seconda dell'e-mail inviata. Sono stati esposti circa 5.001 indirizzi e-mail di utenti dell'app MiniMed Mobile in tutto il mondo, di cui 732 in Italia.	

VIOLAZIONE 2	Mancata indicazione nell'informativa della base giuridica della comunicazione di dati personali dei pazienti interessati a collegare il proprio account personale con quello del professionista sanitario.

Centro Estetico

Comunicazione di dati

Violazione obblighi di trasparenza

Trattamento illecito dei dati

Diffusione di dati relativi alla salute; Informativa privacy non conforme; Consenso non conforme

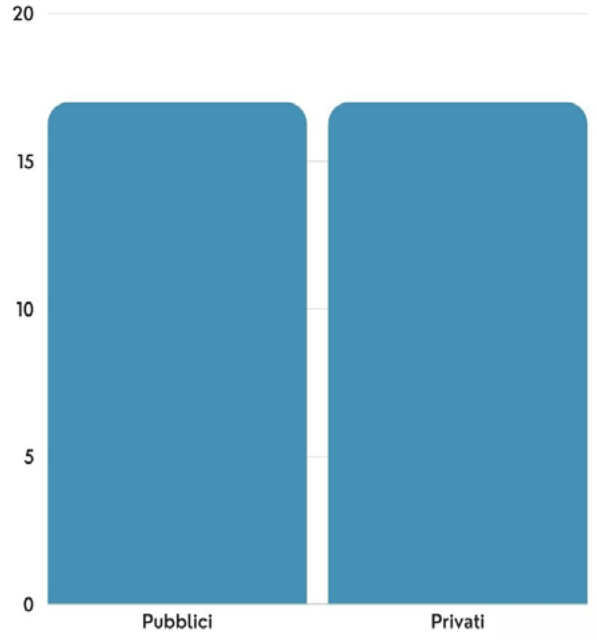
	[doc. web n. 9983210]	
	Centro Estetico - David S.r.l. (Centro estetico Dvora)	
	11 Gennaio 2024	Milano (MI)
	€ 8.000	
Origine della sanzione	Reclamo	
Parametro impattato	**RISERVATEZZA**	
VIOLAZIONE 1	Diffusione sul social media Instagram, nel profilo pubblico "DvoraAncona" della Società David S.r.l. (Centro Estetico Dvora), di un video in cui il reclamante è stato ripreso durante una procedura di medicina estetica (Rinoplastica non chirurgica) effettuata dalla dott.ssa Ancona, legale rappresentante della Società David S.r.l. cui fa capo il Centro Estetico Dvora.	
VIOLAZIONE 2	L'informativa utilizzata dal titolare, nella sezione rubricata "Finalità del trattamento", reca un generico riferimento "alla pubblicazione di articoli su social media e magazine" non specificando che sarebbero stati diffusi dati sulla salute dell'interessato sul profilo pubblico "DvoraAncona" di Instagram della Società, senza alcuna pseudonimizzazione degli stessi.	

VIOLAZIONE 3	Non può ritenersi validamente prestato il consenso c.d. "tacito" dell'interessato in quanto la circostanza che la prestazione sanitaria a cui l'interessato si stava sottoponendo è stata registrata non all'insaputa dell'interessato, non equivale ad aver acquisito dallo stesso un consenso informato, specifico ed esplicito circa le modalità con cui i dati oggetto della stessa ripresa sarebbero stati trattati e, nel caso di specie, addirittura diffusi su un canale social.

Grafici riassuntivi

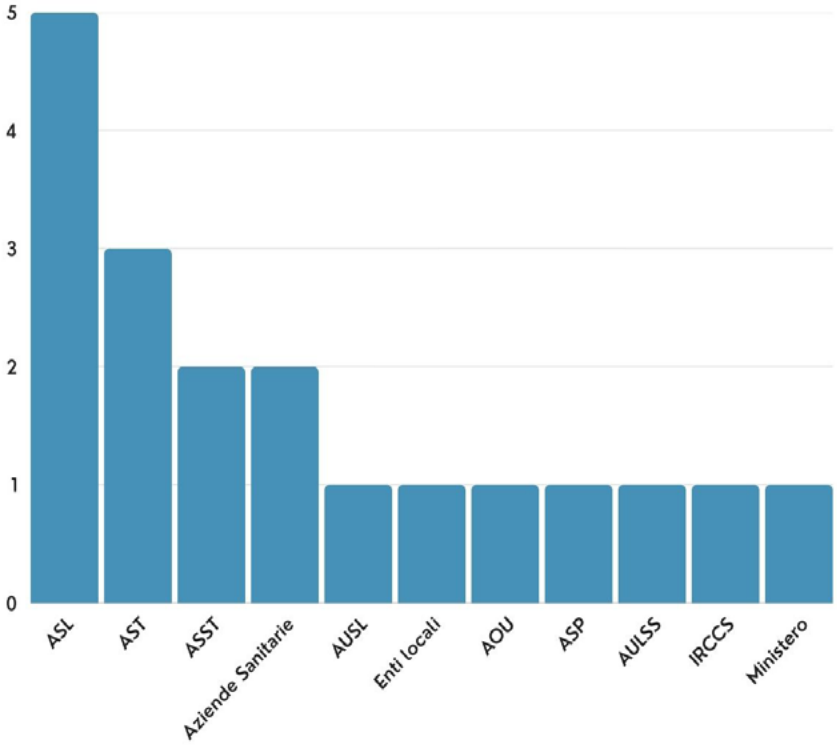
DESTINATARI DELLE SANZIONI

Sanzioni privacy in sanità nel 2024



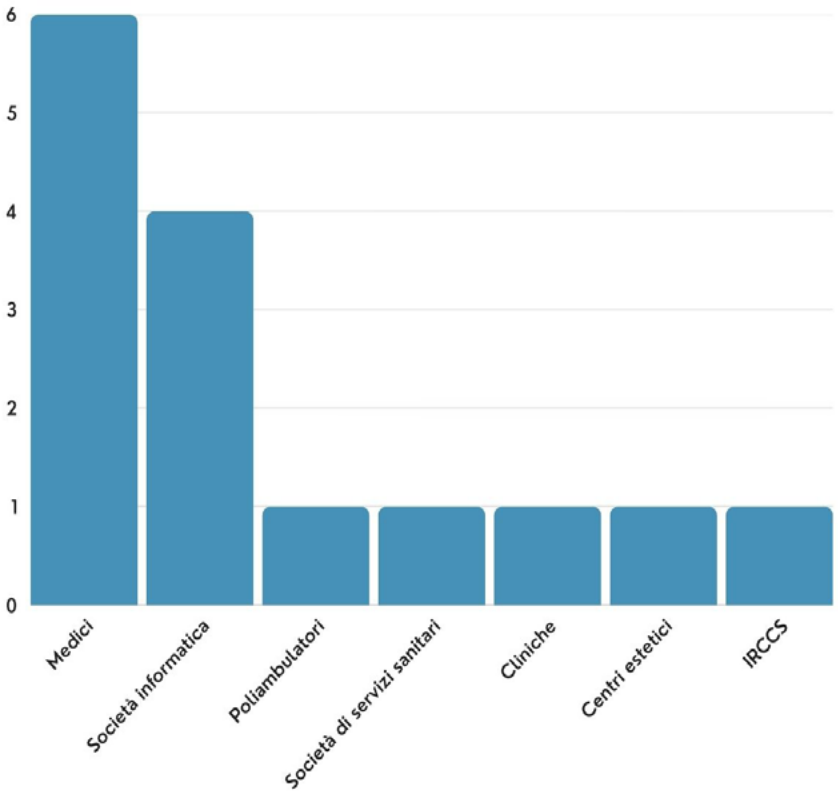
DESTINATARI DELLE SANZIONI - SOGGETTI PUBBLICI

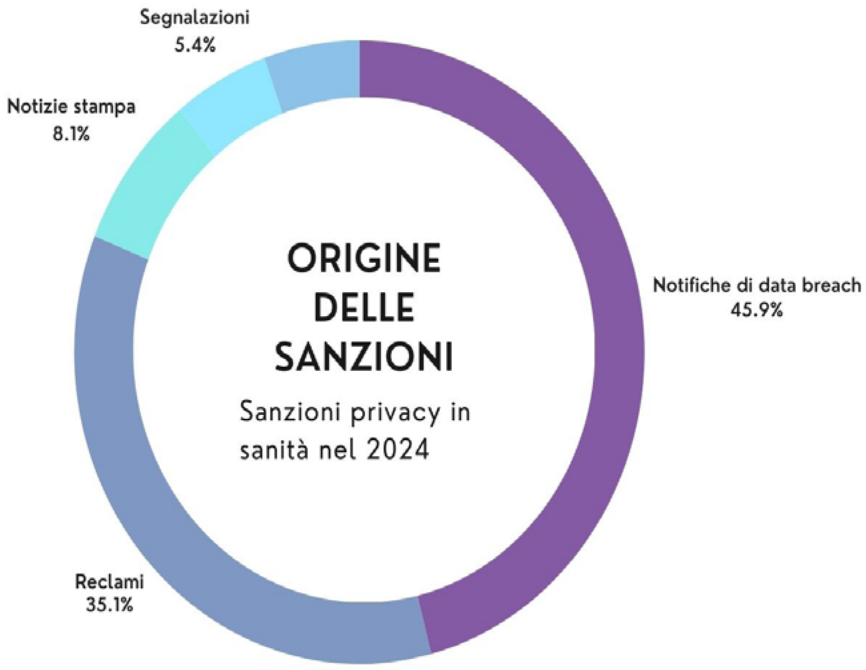
Sanzioni privacy in sanità nel 2024



DESTINATARI DELLE SANZIONI - SOGGETTI PRIVATI

Sanzioni privacy in sanità nel 2024





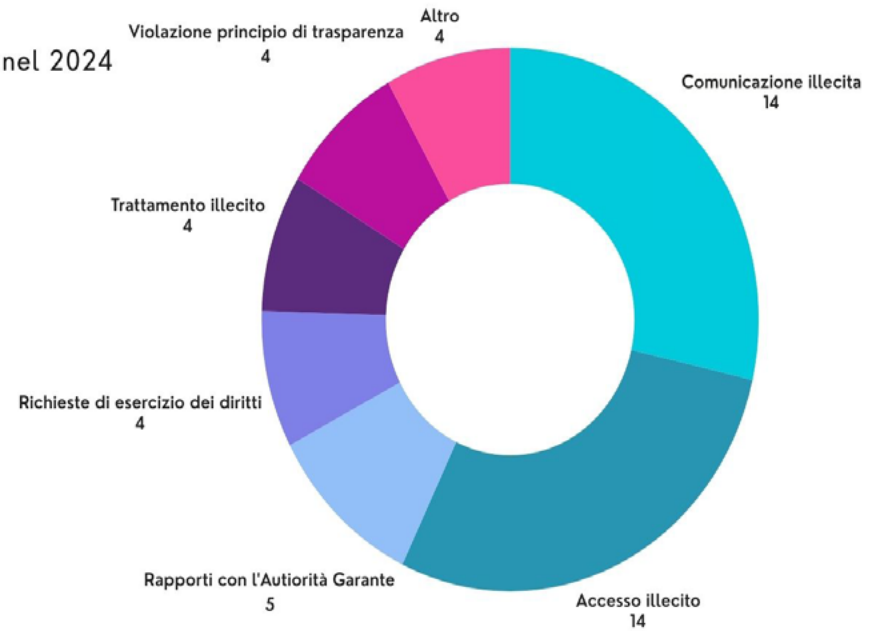
OGGETTO DELLE SANZIONI

Sanzioni privacy in sanità nel 2024



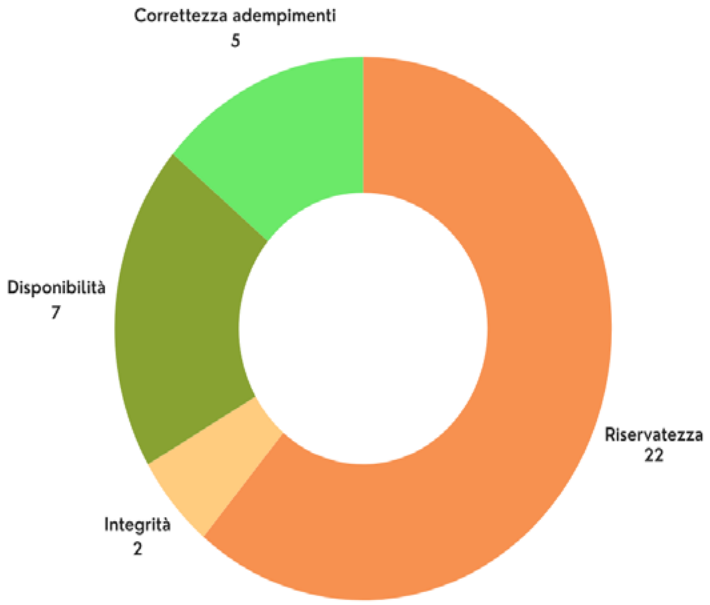
LE CATEGORIE DI VIOLAZIONI COMMESSE

Sanzioni privacy in sanità nel 2024



PARAMETRO IMPATTATO

Sanzioni privacy in sanità nel 2024

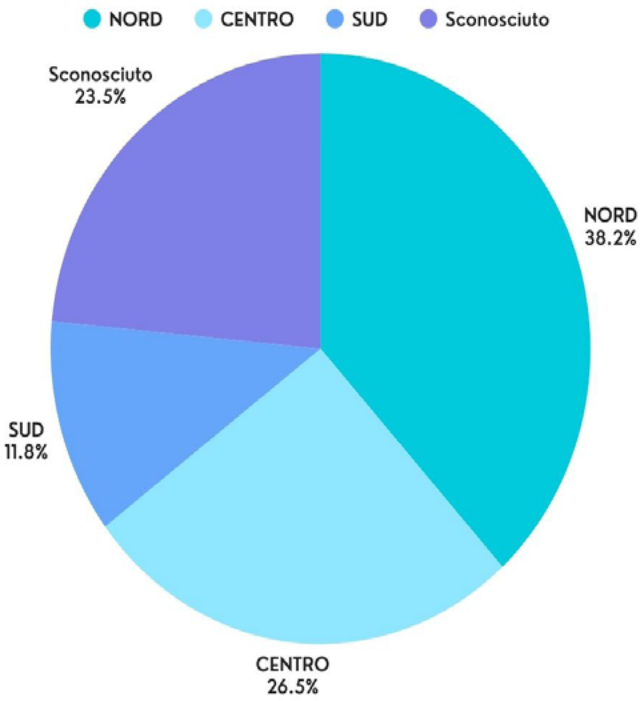




LOCALIZZAZIONE GEOGRAFICA DELLE SANZIONI

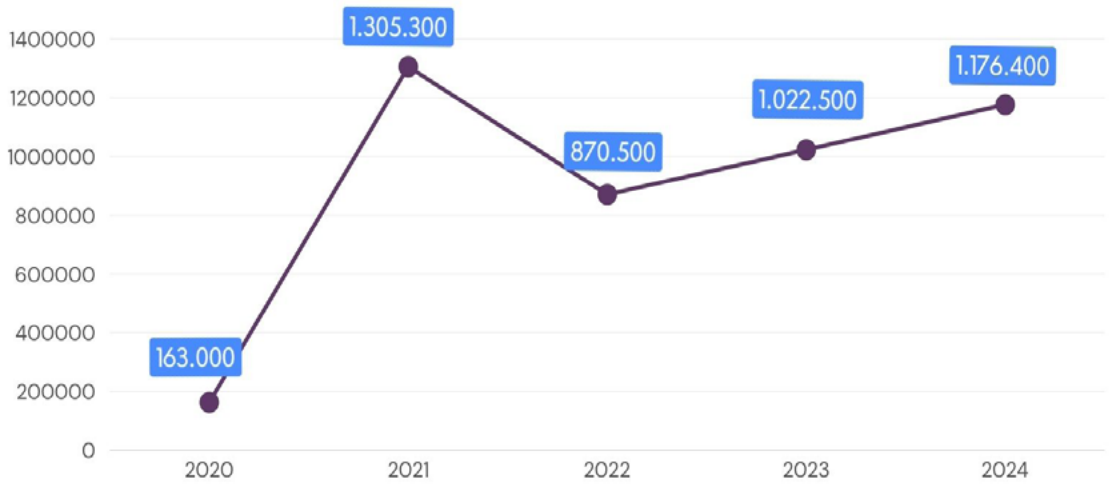
Sanzioni privacy in sanità nel 2024

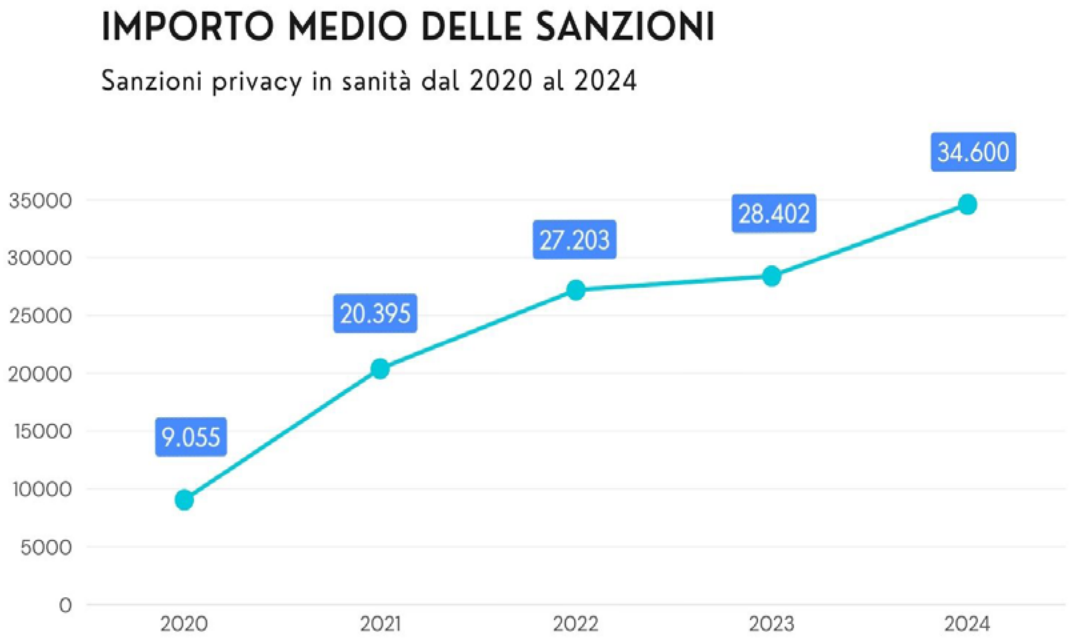




IMPORTO TOTALE DELLE SANZIONI

Sanzioni privacy in sanità dal 2020 al 2024




IMPORTO MEDIO DELLE SANZIONI
Sanzioni privacy in sanità dal 2020 al 2024
35000
30000
25000
20000
15000
10000
5000
0
9.055
20.395
27.203
28.402
34.600
2020
2021
2022
2023
2024

L'AUTRICE



avv. Maria Livia Rizzo

ml.rizzo@studiolegalestefanelli.it

L'avvocata Maria Livia Rizzo svolge attività di consulenza legale in materia di protezione dei dati personali e cybersecurity per strutture sanitarie pubbliche e private, enti di ricerca, società farmaceutiche e di medical device. Si occupa della conformità di organizzazioni e progetti innovativi di health tech alle normative in materia di data protection e sicurezza delle infrastrutture digitali, e fornisce assistenza nell'implementazione dei relativi modelli di governance.

È referente del Dipartimento Privacy dello Studio Legale Stefanelli&Stefanelli.

Laureata in Giurisprudenza presso l'Università di Bologna con il massimo dei voti, ha conseguito il Dottorato di ricerca in Diritto e Nuove Tecnologie presso il CIRSFID (Università di Bologna) dove ha svolto attività di ricerca come Assegnista e ricoperto il ruolo di Tutor didattico del Master in Trattamento dei dati personali e Privacy Officer. Ha conseguito presso l'Università degli Studi di Milano Statale i Corsi di perfezionamento in "Data Protection and Data Governance: la Cybersecurity", "Big data, Artificial Intelligence e Piattaforme", "Coding for Lawyers e Legal Tech: Programmazione per giuristi, Smart Contract e Legal Design" e "Criminalità informatica e Investigazioni digitali: il fattore umano".

È stata Cultrice della materia in Informatica Giuridica e in Medicina Legale presso la Scuola di Giurisprudenza dell'Università di Bologna, titolare del Modulo didattico "Regulatory and economic aspects" (SSD IUS/10) del Master in Innovation in eXtended Reality (MIXR) dell'Università di Bologna A.A. 2019/2020 e Peer reviewer del Journal of Medical Ethics – British Medical Journal.

Ha svolto docenze in Corsi di Dottorato di ricerca, Master universitari e Corsi di Laurea in varie Università italiane, ha partecipato a roundtable presso il Joint Research Centre della Commissione Europea ed è stata relatrice in conferenze e convegni dedicati a temi di diritto, salute e tecnologia.

È autrice di pubblicazioni su riviste scientifiche e volumi collettanei, oltre che di contributi di carattere divulgativo.

È Socio Fondatore e Vice Presidente dell'Associazione italiana di Stampa 3D in Medicina - IDBN (Italian Digital Biomanufacturing Network) e componente del Comitato scientifico della I e II edizione del relativo Congresso Nazionale.

Studio Legale Stefanelli&Stefanelli

www.studiolegalestefanelli.it

www.privacygdpr.it

Bologna: Via Azzo Gardino 8/A

Roma: Palazzo Marignoli - Piazza di San Silvestro, 8

Milano: Via Nino Bixio, 31

Venezia: Sestiere Castello 2388

Edizione: Ottobre 2024

Tutti i diritti di traduzione, di riproduzione, di adattamento, totale o parziale, con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche) sono riservati. Ogni permesso deve essere dato per iscritto dall'editore.