AmTrust Assicurazioni

I requisiti privacy applicati alla documentazione sanitaria

Cagliari – 14 giugno 2023

AmTrust Assicurazioni

Marica Piccioli

Head of Compliance & DPO

Agenda

- Quadro normativo
- Principali definizioni
- Soggetti
- Liceità del trattamento
- Documentazione sanitaria
- Sanzioni

AmTrust Assicurazioni

AmTrust Assicurazioni

1

Sezione 1:
Quadro normativo

Quadro normativo di riferimento

AmTrust Assicurazioni

Regolamento UE 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

Effettiva applicazione: 25 Maggio 2018

D. Lgs. 196/2003 (c.d. Codice Privacy) recante il «Codice in materia di protezione dei dati personali», **in particolare tutto il Titolo V** – Trattamento dei dati personali in ambito sanitario e d.lgs.101/2018 di adeguamento del Codice.

Garante Privacy:

- Provvedimento 7/3/2019 **–** chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario;
- **Provvedimento 5/6/2019 – prescrizioni relative al trattamento di categorie particolari di dati**.

Legge n.24/2017 (c.d. Legge Gelli) all'articolo, comma 1 recita: «*Le prestazioni sanitarie erogate dalle strutture pubbliche e private sono soggette **all'obbligo di trasparenza**, nel rispetto del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n.196*»

AmTrust Assicurazioni

2

Sezione 2:
Principali definizioni

AmTrust Assicurazioni

PRINCIPALI DEFINZIONI

Dato Personale

Dato personale: **qualsiasi informazione** riguardante una **persona fisica** identificata o identificabile («interessato»); è identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati relative alla salute

Dati relativi alla salute: i dati personali attinenti alla **salute fisica o mentale** di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative al suo stato di salute.

Categorie particolari di dati

Categorie particolari di dati: **dati idonei a rivelare lo stato di salute**, la vita sessuale, l'origine razziale o etnica, le convinzioni religiose dell'interessato, nonché dati genetici.

Trattamento

Trattamento: **qualsiasi operazione** o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Consenso al trattamento

Consenso dell'interessato: qualsiasi manifestazione di volontà, libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile che i dati personali che lo riguardano siano oggetto di trattamento.

AmTrust Assicurazioni

3

Sezione 3:
Soggetti

Soggetti

1. **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali

2. **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

3. **Incaricato al trattamento:** la persona fisica espressamente autorizzata al trattamento da parte del Titolare, che ha ricevuto debite istruzioni operative

4. **Interessato:** il soggetto a cui si riferiscono i dati personali oggetto di trattamento

5. **DPO:** Responsabile della protezione dei dati (**Data Protection Officer**)

Esempi

AmTrust Assicurazioni

1 **Titolare del trattamento**

- Azienda regionale della salute (ARES)
- Azienda regionale emergenza urgenza (AREUS)
- AOU Cagliari
- AOU Sassari
- ASL Gallura
- AmTrust Assicurazioni S.p.A.

Estrapolati dal sito di ARES

2 **Responsabile del trattamento**

- Società di archiviazione della documentazione clinica
- Società di elaborazione paghe e contributi
- Società di gestione del sito web/applicazione

3 **Incaricato del trattamento**

- Personale e operatori dell'ospedale
- Personale della Compagnia assicurativa

4 **Interessato**

- Paziente
- Danneggiato
- Dipendente dell'ospedale

5 **Responsabile della protezione Dati (DPO)**

- Soggetto interno/esterno (esempio: dpo@aousassari.it)

AmTrust Assicurazioni

4

Sezione 4:
Fondamenti di liceità del trattamento

Principi Applicabili
Liceità del trattamento

AmTrust Assicurazioni

Ogni trattamento di dati personali deve trovare fondamento in un'idonea base giuridica.
In particolare, **l'articolo 6 «Liceità del trattamento»**, individua le diverse **basi giuridiche** in base alla quale il Titolare può trattare i dati del paziente.
Quali ad esempio:

- il consenso dell'interessato,
- esecuzione di un contratto,
- per adempiere un obbligo di legge,
- legittimo interesse.

I dati sono:

- Trattati in modo **lecito**, corretto e trasparente
- Raccolti per **finalità determinate**, esplicite e legittime
- Adeguati, pertinenti e limitati a quanto necessario
- Esatti e, se necessario, aggiornati
- **Conservati** per un arco di tempo non superiore al conseguimento delle finalità per i quali sono trattati
- Trattati in modo da garantire un'adeguata sicurezza dei dati personali

AmTrust Assicurazioni

5

Sezione 5:
Documentazione sanitaria – quali obblighi per il titolare

Quali obblighi in capo al Titolare?

AmTrust Assicurazioni

1

Al paziente deve essere fornita una esaustiva **informativa privacy** *(quali dati personali vengono trattati, perché, come e per quanto tempo vengono conservati, scritta con un linguaggio semplice e chiaro)*

Nell'informativa è fondamentale definire chiaramente:

- chi è il soggetto che raccoglie e tratta i dati (il Titolare);
- I dati del responsabili della protezione dei dati (DPO);
- le finalità del trattamento;
- la base giuridica sulla quale si basa il trattamento dei dati e quali sono i casi in cui è necessario il consenso esplicito dell'interessato al trattamento stesso;
- il periodo di conservazione delle informazioni;
- come viene svolto il trattamento dei dati;
- se i dati sono, o possono, essere trasferiti a soggetti terzi e nel caso a quali soggetti;
- se i dati possono essere comunicati a soggetti terzi (ad esempio i parenti dell'interessato);
- i diritti dell'interessato.

Ogni volta che le finalità cambiano il Regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Esempi di diverse tipologie «informativa privacy»

AmTrust Assicurazioni

INFORMAZIONI AI SENSI DEGLI ARTT. 13 E 14 DEL GDPR

- Informazioni privacy per i pazienti (pdf - 560 KB)
- Modulo per l'esercizio di diritti in materia di protezione dei dati personali (pdf - 82 KB)
- Informazioni privacy per i fornitori (pdf - 158 KB)
- Informazioni Privacy per consulenti e collaboratori finalizzate alla verifica dell'assenza di cause di inconferibilità e di conflitto di interesse (pdf - 189 KB)
- Informazioni privacy - Banca delle membrane amniotiche (pdf - 81 KB)
- Informativa privacy - Programma Screening Prevenzione Serena (agg. il 29/10/2019) (pdf - 243 KB)
- Informativa privacy - Emergenza territoriale 118 (pdf - 25 KB)
- Informazioni privacy - Procreazione assistita (agg. il 14/10/2021) (pdf - 202 KB)
- Informativa privacy - Dossier Sanitario Elettronico (DSE) (pdf - 273 KB)
- Informativa privacy - Servizio di Prenotazione CUP (pdf - 426 KB)
- Informazioni privacy - Videosorveglianza (pdf - 817 KB)
- Informativa privacy - Banca del Latte umano donato (BLUD) (pdf - 385 KB)
- Informazioni privacy - Controllo Green Pass (agg. il 22/12/2021) (pdf - 288 KB)
- Informazioni privacy ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 per trattamento dei dati personali relativi alla donazione di sangue (agg. al 20/12/2022) (pdf - 141 KB)

Ultimo aggiornamento (Venerdì 23 Dicembre 2022 11:41)

Informative Privacy pubblicate sul sito di un ospedale piemontese

Esempi di testi di informative privacy di strutture sanitarie

AmTrust Assicurazioni

	PERCHÉ VENGONO TRATTATI I SUOI DATI PERSONALI E QUAL È LA CONDIZIONE CHE RENDE LECITO IL TRATTAMENTO?		PER QUANTO TEMPO CONSERVIAMO I DATI PERSONALI?
A)	Per poter esercitare le **attività di prevenzione, diagnosi, cura e riabilitazione**, ivi compresi i servizi diagnostici, terapeutici, di laboratorio, le prestazioni specialistiche ambulatoriali, di ricovero ospedaliero, di continuità assistenziale post dimissione.	Le condizioni che rendono lecito il trattamento sono: • l'art. 6, comma 1 lett. b del Regolamento, per quanto riguarda i dati comuni (esecuzione della Sua richiesta di accedere alle prestazioni erogate dalla struttura) • l'art. art. 9, c. 2 lett. h per quanto riguarda le categorie particolari di dati (finalità di diagnosi, assistenza o terapia sanitaria)	**Le cartelle cliniche, unitamente ai relativi referti, sono conservate illimitatamente** poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario. (Circolare Ministero Sanità n. 61 del 1986, n. 900 del 1996); 5 anni per i certificati di idoneità alla attività sportiva agonistica (art. 5 D.M. 18/02/1982); documentazione iconografica radiologica 10 anni (art. 4 D.M. 14/02/1997).
B)	Per svolgere **attività amministrative e contabili connesse** all'erogazione della prestazione sanitaria, ad esempio per gestire le prenotazioni, l'accettazione del paziente, la compilazione di cartelle cliniche e		

2. Finalità del trattamento

Il trattamento dei dati raccolti avverrà per finalità di diagnosi, cura, riabilitazione, prevenzione e ricerca (in quest'ultimo caso resi assolutamente anonimi), e comunque per il conseguimento delle finalità istituzionali attribuite a questa Azienda dalla vigente normativa nazionale e regionale ed in particolare dalla L.833/78, dal D.Lgs.502/92 e s.m.i. dalle LL.Reg. n.8/95, 10/95, 18/2007 e s.m.i., e dal DPCM 29.11.2001, e per l'assolvimento di specifici obblighi di legge. Il trattamento dei dati potrà avvenire altresì per le finalità indicate all'art.9.2 lett.b, c, f, h, i, j) del GDPR.

I Suoi dati potranno essere trasmessi ad altre Aziende Sanitarie Pubbliche e Case di Cura Private, al Suo medico di famiglia, all'Autorità Giudiziaria e/o di Pubblica Sicurezza, nei casi e nei limiti espressamente previsti dalla legge, ad enti previdenziali ed assistenziali, nonché a quei soggetti ai quali la comunicazione sia obbligatoria per legge, che tratteranno i dati nella loro qualità di autonomi titolari del trattamento. I dati non saranno comunicati ad altri soggetti o trattati per finalità diverse, senza aver acquisito il Suo preventivo consenso. I dati trattati non sono soggetti a diffusione e saranno conservati per i periodi di tempo stabiliti dalle vigenti disposizioni di legge o regolamentari.

3. Modalità di trattamento – Dossier Sanitario Elettronico

Il trattamento dei Suoi dati personali è realizzato per mezzo delle operazioni indicate all'art. 4 n.2) del GDPR e precisamente: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione.

Il trattamento verrà effettuato sia ricorrendo a strumenti informatizzati (ad es. Dossier Sanitario Elettronico DSE) che cartacei

Quali obblighi in capo al Titolare?

AmTrust Assicurazioni

Il Regolamento (art.9, comma 1) **vieta il trattamento** di categorie particolari di dati personali, salvo l'interessato non abbia prestato il proprio consenso

2 Base giuridica - consenso dell'interessato: quando Si e quando NO

NO

E' possibile trattare «**categorie particolari di dati**» in ambito sanitario **SENZA** l'esplicito consenso al trattamento dei dati da parte del paziente/interessato purché (Art.9, comma 2, lettera h) e comma 3):

a) *il trattamento è essenziale per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute (**c.d. finalità di cura**); **E***
b) *Il trattamento è effettuato da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza*

SI

E' possibile trattare «**categorie particolari di dati**» in ambito sanitario **SOLO** con l'esplicito consenso al trattamento dei dati da parte del paziente/interessato, in tutti gli altri casi ad esempio:

a) *Trattamento dati genetici*
b) *Consultazione del Fascicolo sanitario elettronico;*
c) *Dossier sanitario elettronico;*
d) *Consegna del referto on line;*
e) *Utilizzo di app mediche (che non siano per la telemedicina);*
f) *Finalità promozionali o commerciali*

Approfondimento sul «consenso dell'interessato»

AmTrust Assicurazioni

Caratteristiche del consenso

- Libero
- Specifico
- Esplicito
- Informato
- Inequivocabile
- Revocabile

Il consenso dei minori è valido, in Italia, a partire dai 14 anni (in conformità con la normativa nazionale): prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.
Il Regolamento stabilisce l'età a 16 anni, ma lo Stato italiano ha derogato tale limite; il Regolamento richiede il consenso di chi esercita la «responsabilità genitoriale», non sempre il titolare della responsabilità genitoriale è il genitore naturale del minore e che la responsabilità genitoriale può essere detenuta da più parti che possono comprendere tanto persone fisiche quanto persone giuridiche.

Quali obblighi in capo al Titolare?

AmTrust Assicurazioni

3 Tempi di conservazione

Qualora non siano fissati da specifiche norme, spetta al Titolare definirli in base alla finalità del trattamento. In ogni caso, devono essere indicati nell'informativa.
Specifiche norme:

- La **Cartella Clinica**, unitamente ai relativi referti, è conservata **illimitatamente** poiché rappresenta un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario (Circolare Ministero Sanità n.61 del 1986, n.900 del 1996, chiarimenti del Garante Privacy n.9091942 del 7 marzo 2019)
- **Documentazione iconografica radiologica**: 10 anni (art. 4 d.m. 14 febbraio 1997)
- La documentazione inerente gli accertamenti effettuati nel corso delle visite per il rilascio del **certificato di idoneità all'attività sportiva agonistica**, che deve essere conservata, a cura del medico visitatore, per almeno 5 anni (art. 5, D.M. 18/02/1982)

4 Responsabile della Protezione dei dati (Data Protection Officer – DPO)

La nomina di un DPO è obbligatoria per un'azienda sanitaria appartenente al SSN, sia in relazione alla natura giuridica di «organismo pubblico», sia in quanto le attività principali di titolare consistono nel trattamento su larga scala dei dati relativi alla salute.
Il Garante ritiene che anche gli ospedali privati, le case di cura e le residenze assistenziali (RSA) possano generalmente rientrare nel concetto di larga scala e quindi obbligate alla nomina di un DPO.

Quali obblighi in capo al Titolare?

AmTrust Assicurazioni

5

Registro dei trattamenti e valutazione di impatto (DPIA)

Il titolare e i responsabili del trattamento devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno della struttura, indispensabile per ogni **valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica.

Misure di sicurezza

6

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento.
Il personale che tratta i dati, rigorosamente autorizzato e preferibilmente con profili specifici di accesso ai dati in relazione ai loro ruoli, deve essere opportunamente istruito.

Documentazione sanitaria – Esempi concreti

A partire dal 2013, la cartella clinica può essere conservata anche solo in formato elettronico

Cartella clinica

La cartella clinica è l'insieme dei documenti che raccolgono tutte le informazioni che riguardano le condizioni del paziente, dall'ingresso in struttura fino alle sue dimissioni.

- **Unico** Titolare del trattamento (ad esempio Ospedale X per un solo ricovero)
- **E' sempre** necessaria l'informativa
- Art.92 del Codice Privacy: la cartella clinica deve essere redatta e conservata adottando opportuni accorgimenti per assicurare la comprensibilità dei dati

CONSENSO DEL PAZIENTE

- NON è necessario il consenso del paziente
- Senza consenso il paziente può ritirare il referto in formato cartaceo presso la struttura in cui è stato svolto l'esame

- E' necessario il consenso del paziente (Linee Guida del Garante Privacy del 2015)

Dossier sanitario

Il Dossier sanitario elettronico (DSE) è lo strumento che raccoglie informazioni sulla salute del paziente per documentare, negli anni, la storia clinica presso una singola struttura.

- **Unico** Titolare del trattamento (ad esempio Ospedale X per molteplici ricoveri)
- **E' sempre** necessaria l'informativa

Documentazione sanitaria – Esempi concreti

AmTrust Assicurazioni

Fascicolo sanitario

Il Fascicolo sanitario elettronico (FSE) è l'insieme di dati e documenti digitali di tipo sanitario e sociosanitario, che raccontano la storia clinica del paziente provenienti da strutture sanitarie, prevalentemente operanti nel medesimo ambito territoriale.

- **Molteplici** Titolare del trattamento (ad esempio Ospedale X,Y e Z per molteplici ricoveri, medico curane)
- **E' sempre** necessaria l'informativa

CONSENSO DEL PAZIENTE

Circolare MEF e Ministero della Salute del 17/2/2021

- Dal 19/5/2020 è stato eliminato il consenso all'alimentazione per la creazione e attivazione del FSE di ciascun assistito
- Consenso necessario invece la consultazione del FSE per finalità di cura (c.d. «consenso alla consultazione») -> la consultazione non è riferibile a finalità di cura e soprattutto possono accedere diversi titolari

- Il paziente deve prestare il proprio consenso per poter ricevere il referto on-line
- Senza consenso il paziente può ritirare il referto in formato cartaceo presso la struttura in cui è stato svolto l'esame

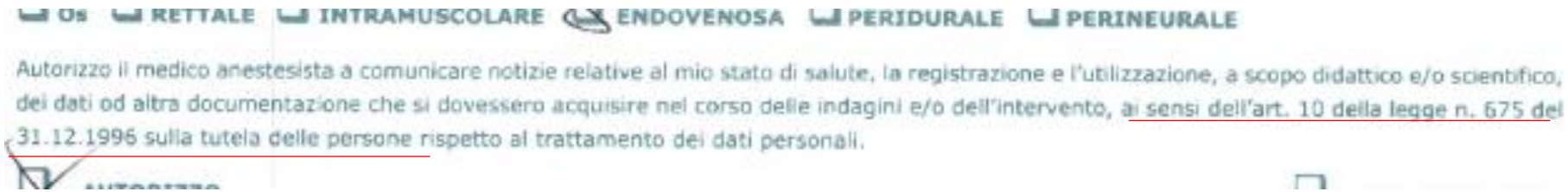
Referti on-line

Servizi che consentono al paziente di accedere al «referto online» inteso come la relazione scritta rilasciata dal medico sullo stato clinico del paziente dopo un esame clinico o strumentale, con modalità informatica.

- **Unico** Titolare del trattamento (ad esempio Ospedale X)
- **E' sempre** necessaria l'informativa

Cosa NON mettere nella cartella clinica o nel consenso informato

AmTrust Assicurazioni



La forma diventa sostanza

Domande frequenti

AmTrust Assicurazioni

Cartella Clinica digitale: permette un accesso rapido, il Titolare deve sicuramente svolgere una DPIA e verificare l'ubicazione del fornitore del servizio e del Cloud (esempio che non sia in un paese terzo, tipo Cloud Microsoft ubicato in USA ovvero fuori dall'Unione Europea)

Rilascio/presa visione della cartella clinica: all'interessato. A soggetti terzi solo con richieste motivate e documentate (art.92 Codice Privacy)

Rilascio informazioni sullo stato di salute del paziente: solo all'interessato. E' possibile fornire informazione a terzi (familiari, congiunti, etc.) solo con esplicito consenso dell'interessato

E' necessario il consenso al trattamento per finalità di ricerca medica, biomedica ed epidemiologica?: NO, ma solo se la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'UE (art.110 codice privacy)

Come dimostro di avere raccolto il consenso?: firma su un modulo cartaceo, registrazione vocale, per e-mail, firma elettronica, flag via sito web

Rischi e nuovi fenomeni

Attacchi Cyber

Ha come primo effetto la violazione della sicurezza dei dati (*data breach*) – Esempi recenti: Spallanzani, San Camillo, ASL 1 Regione Abruzzo, Ospedale di Alessandria

PNRR – Missione 6 Salute e DM77

Collaborazione territoriale e telemedicina

Intelligenza Artificiale

I dispositivi medici dotati di IA sono da considerarsi ad alto rischio
(secondo la proposta di regolamento dell'IA)

Novità normative

DORA: Digital Operationl Resilience Act

Sanzioni

AmTrust Assicurazioni

Il regolamento (GDPR) prevede due livelli di sanzioni

1 Fino a **10.000.000 o al 2%** del fatturato mondiale totale annuo dell'esercizio precedente

- Designazione DPO e adempimenti connessi
- Valutazione d'impatto (DPIA)
- Mansioni e responsabilità del responsabile del trattamento
- Accordo tra contitolari per la determinazione delle rispettive responsabilità
- Registro delle attività di trattamento
- Misure di sicurezza adeguate
- Notifica al Garante di una violazione di dati personali
- Comunicazione all'interessato di una violazione dei dati personali

2 Fino a **20.000.000 o al 4%** del fatturato mondiale totale annuo dell'esercizio precedente

- Principi generali applicabili al trattamento
- Condizioni di liceità del trattamento, incluso il consenso
- Trattamento di categorie particolari di dati
- Rispetto dei diritti dell'interessato
- Principi per il trasferimento dei dati extra UE
- Norme nazionali in tema di rapporti di lavoro

Oltre a quanto previsto dal regolamento, il Codice Privacy prevede sanzioni anche di carattere penale.

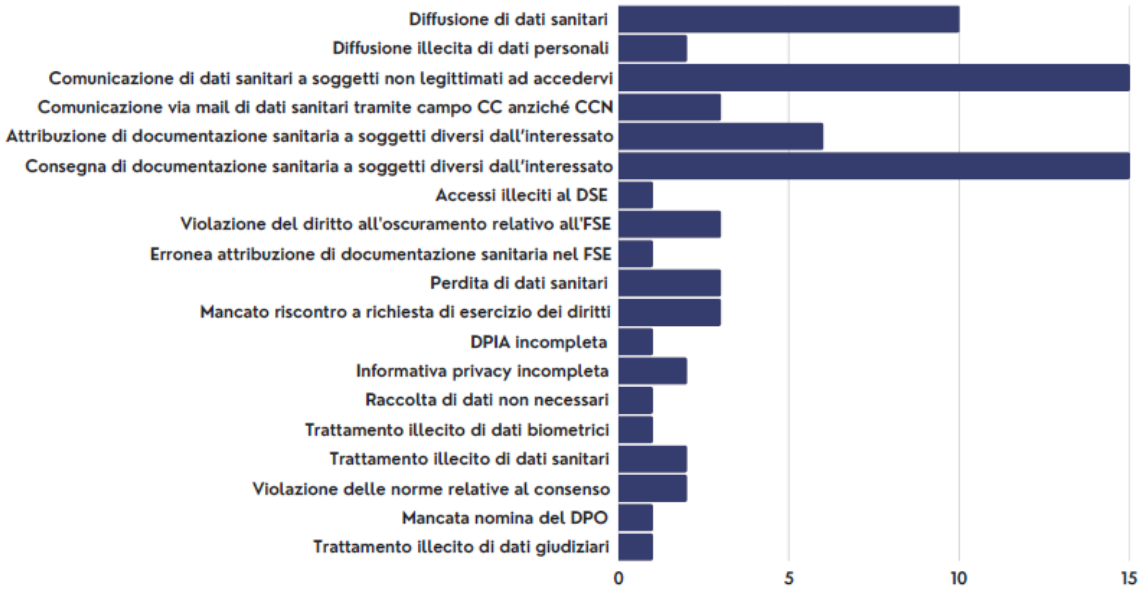
- Art. 167, comma 2 – Trattamento illecito dei dati: «*Salvo il fatto costituisca più grave reato,* ***chiunque****, al fine di trarre per se' o per altri profitto ovvero di arrecare danni all'interessato… omissis…* ***è punito con la reclusione da 1 a 3 anni***»

Garante Privacy: sanzioni 2021

AmTrust Assicurazioni

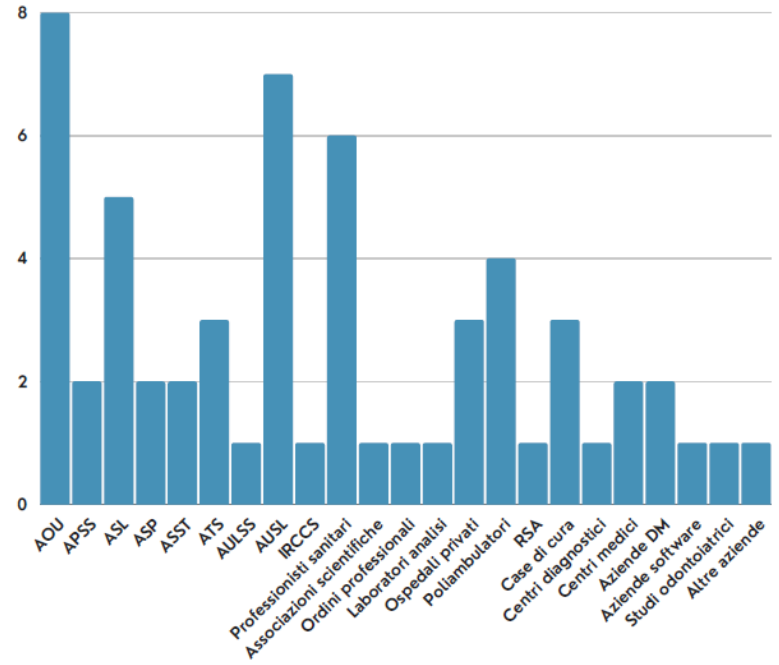
OGGETTO DELLE SANZIONI

Sanzioni privacy in sanità nel 2021



DESTINATARI DELLE SANZIONI

Sanzioni privacy in sanità nel 2021



Per un totale di 1.179.300 euro

Grazie

www.amtrust.it