AIIC 2024 ROMA

PRIVACY E SICUREZZA D'USO DEI DISPOSITIVI MEDICI

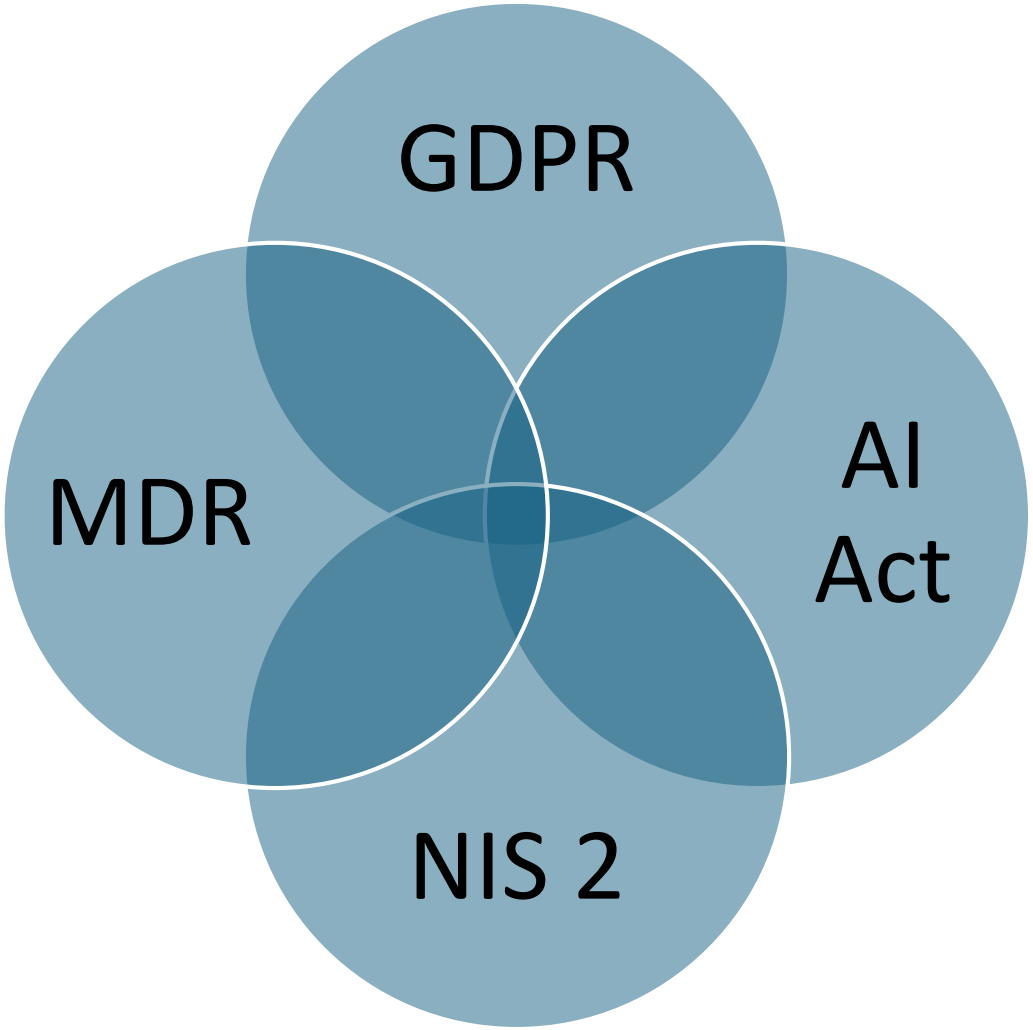
DOROTEA ALESSANDRA DE MARCO

AIIC associazione italiana ingegneri clinici

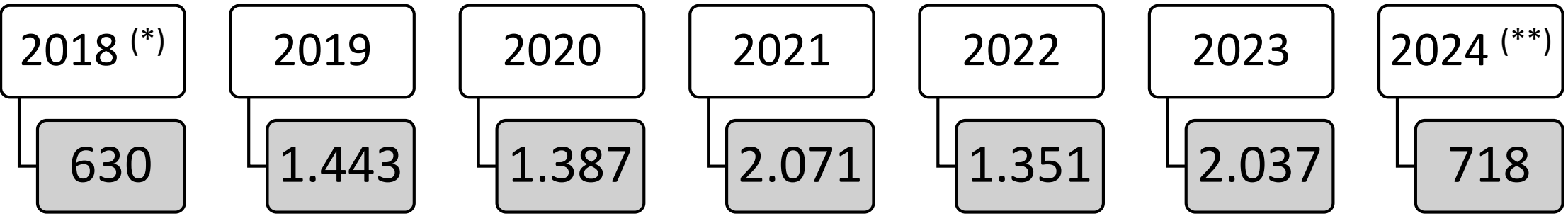
Agenda

- Contesto
- Data breach
- Problematiche
- Greenbone report
- Esempi di misure DPbDD
- Provvedimento Grandi apparecchiature

Contesto



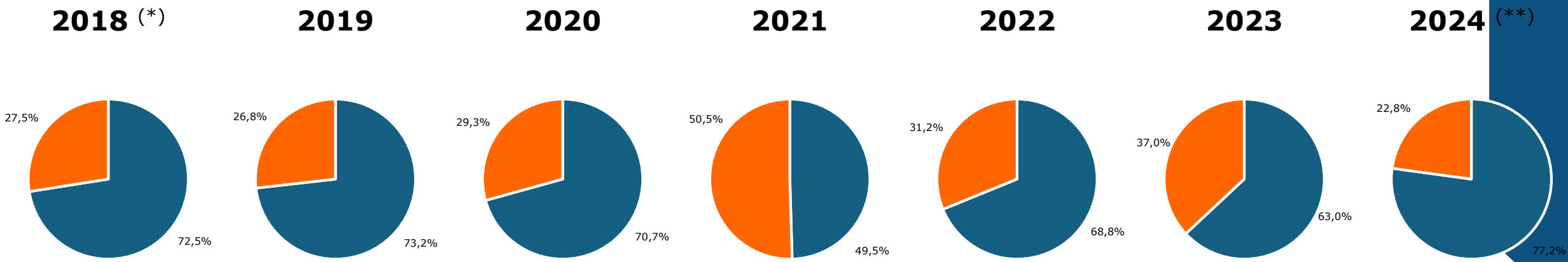
Data breach



(*) dal 25 maggio
(**) fino al 30 aprile

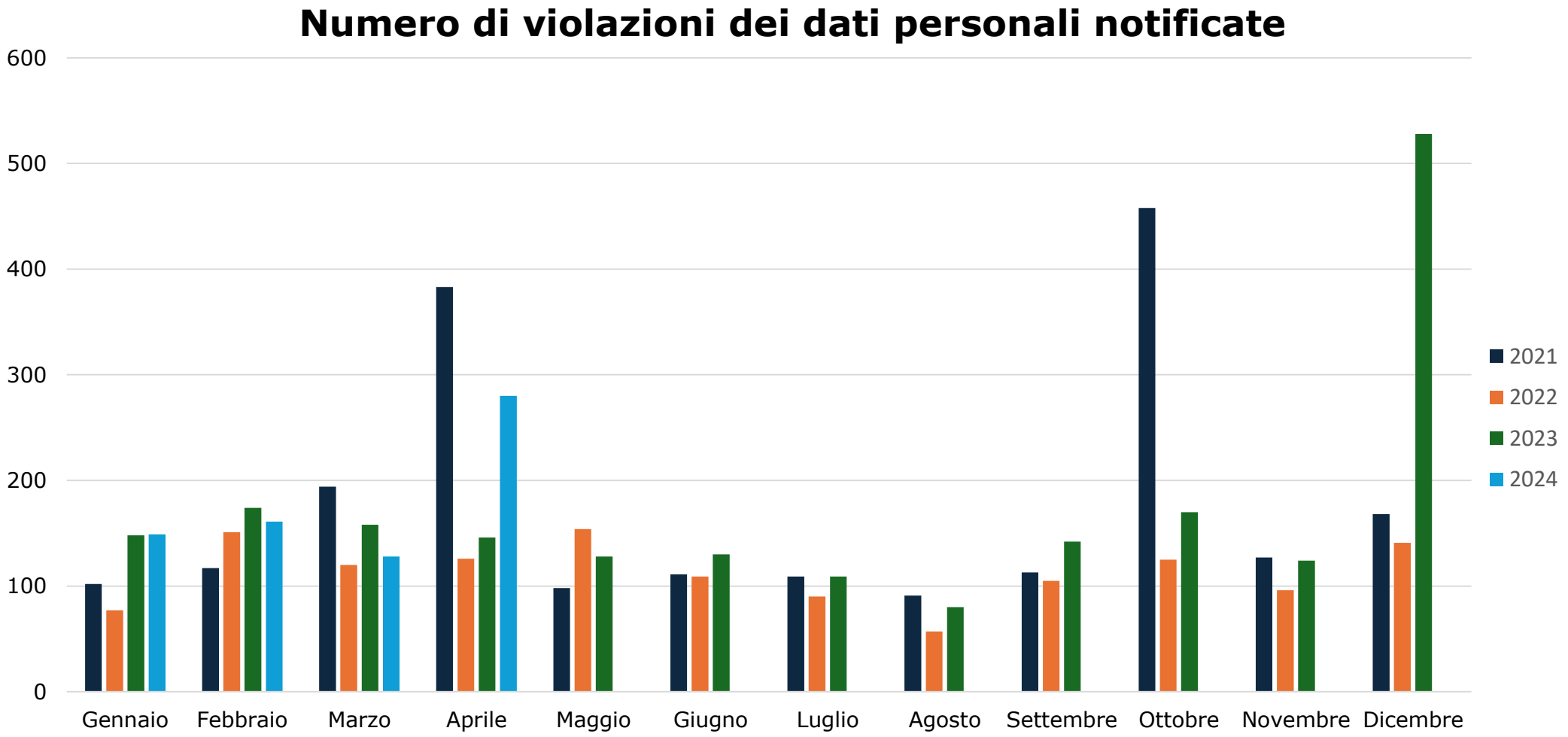
Data breach

Percentuale di violazioni dei dati personali notificate per tipologia di titolare del trattamento

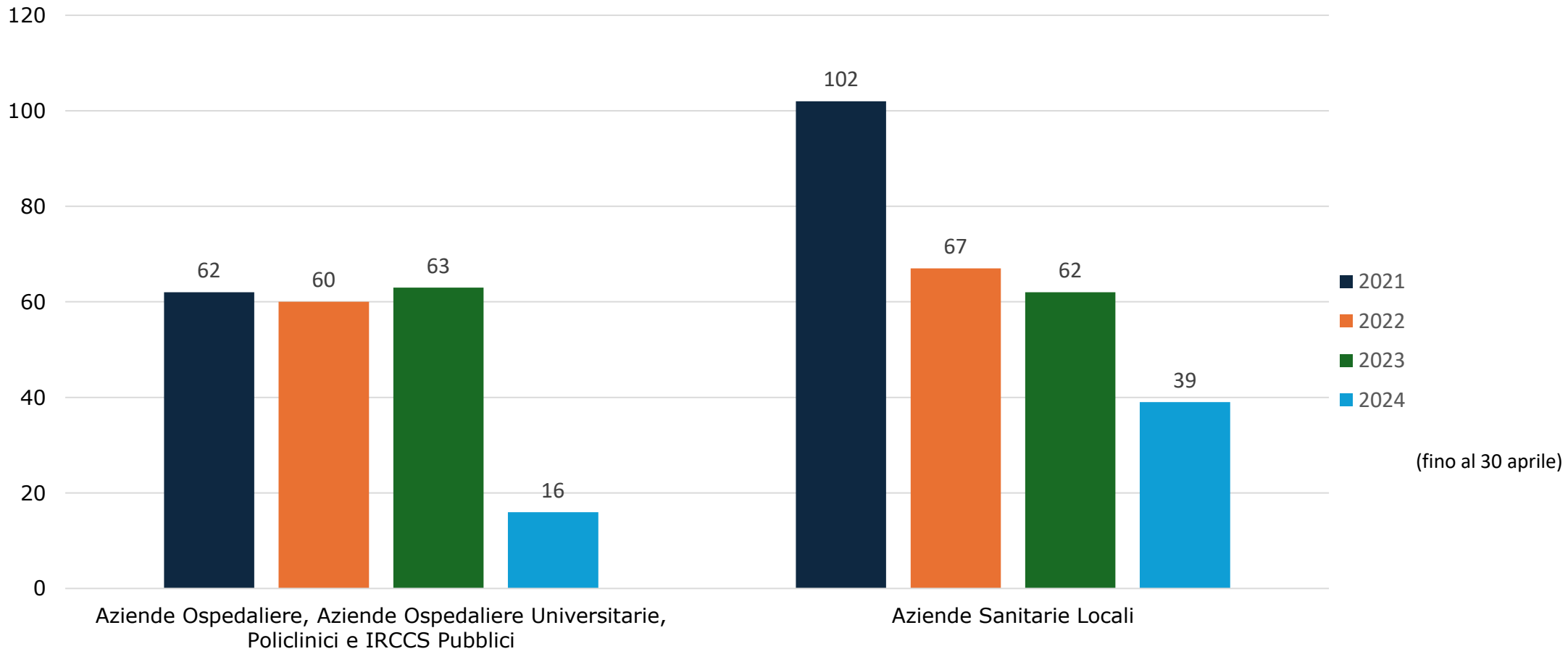


(*) dal 25 maggio
(**) fino al 30 aprile

Data breach


Numero di violazioni dei dati personali notificate
600
500
400
300
200
100
0
Gennaio
Febbraio
Marzo
Aprile
Maggio
Giugno
Luglio
Agosto
Settembre
Ottobre
Novembre
Dicembre
2021
2022
2023
2024

Data breach



(fino al 30 aprile)

Problematiche

con l’aumento dei dispositivi medici connessi alla rete, come monitor cardiaci e pompe per insulina, cresce il rischio di attacchi informatici che potrebbero compromettere la sicurezza dei pazienti

Gli incidenti in ambito sanitario, classificati perlopiù di gravità elevata mettono a rischio non solo i dati e la privacy dei pazienti ma anche la continuità delle cure e la sicurezza dei dispositivi medici (Fonte rapporto CLUSIT)

Problematiche RIS PACS

cancellazione studi per errore del tecnico	attacchi	Indisponibilità
configurazione archiviazione	ransomware	Black out
formattazione	esfiltrazione (lateral movement)	altro
cancellazione erronea		
bug sw		

Greenbone report

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
Albania	1	200	1.000	-	-
Anguilla	1	2.972	44.850	-	-
Argentina	10	11.824	25.472	-	-
Australia	6	49.922	2.596.469	2.496.260	-
Barbados	1	14	2.800	-	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Brazil	34	643.892	31.110.131	15.141.864	4
Bulgaria	2	27.058	40.977	40.977	-
Canada	5	117.425	6.019.030	980.500	-
Chile	18	226.886	4.218.279	2.794.898	3
China	14	279.928	4.882.722	376.905	-
Colombia	8	55.345	1.155.195	1.114.602	1
Costa Rica	1	3.202	12.808	12.808	1
Cyprus	1	3.459	1.124.175	1.124.175	-
Czech Republic	2	97.997	674.686	-	-
Ecuador	19	81.363	5.308.881	4.621.285	2
Egypt	2	827	124.130	124.130	-
France	7	47.662	5.275.222	2.668.170	-
Germany	6	15.310	2.859.595	1.394.845	-
Greece	2	10.211	2.557.600	2.557.600	-
Guatemala	4	13.012	1.039.241	1.039.241	2
India	96	627.777	105.941.300	104.120.549	6
Iran	2	118.692	1.903.384	1.903.384	-
Italy	10	102.893	5.843.319	1.174.600	-

Information Security Report

Confidential patient data freely accessible on the internet

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- sistema di gestione della sicurezza delle informazioni – occorre disporre di uno strumento operativo per gestire le politiche e le procedure per la sicurezza delle informazioni;
- **analisi del rischio** – valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti delle persone, e contrastare quelli identificati, nonché, ai fini dell'utilizzo nella valutazione dei rischi, sviluppare e gestire una «modellizzazione delle minacce» esaustiva, sistematica e realistica e un'analisi della superficie di attacco riferita al software specifico così da ridurre i vettori di attacco e le opportunità di sfruttare eventuali punti deboli e vulnerabilità;
- **sicurezza fin dalla progettazione** – tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti;

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- **manutenzione – rivedere e verificare periodicamente il software, l'hardware, i sistemi e i servizi, ecc. per scoprire eventuali vulnerabilità dei sistemi di supporto del trattamento**;
- gestione del **controllo degli accessi** – solo il personale autorizzato che ne ha necessità dovrebbe avere accesso ai dati personali necessari ai loro compiti di trattamento. Inoltre, il titolare dovrebbe differenziare i privilegi di accesso del personale autorizzato;
  - limitazione dell'accesso (agenti) – definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie funzioni, e limitare l'accesso di conseguenza;
  - limitazione dell'accesso (contenuto) – nel contesto di ciascuna operazione di trattamento, limitare l'accesso per ogni set di dati ai soli attributi che sono necessari allo svolgimento di tale operazione. Limitare inoltre l'accesso ai dati relativi agli interessati di competenza del rispettivo dipendente;
  - segregazione dell'accesso – definire il trattamento dei dati in modo tale che nessuno necessiti di accedere a tutti i dati raccolti sull'interessato, tanto meno a tutti i dati personali di una categoria specifica di interessati;

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- **trasferimenti sicuri** – i trasferimenti sono protetti da modifiche e accessi non autorizzati e accidentali
- **conservazione sicura** – la conservazione dei dati è protetta da modifiche e accessi non autorizzati. Dovrebbero essere previste procedure per valutare il rischio di conservazione centralizzata o decentrata, e le categorie di dati personali cui si applicano. Alcuni dati potrebbero richiedere misure di sicurezza supplementari rispetto ad altri o l'isolamento da questi ultimi;
- **pseudonimizzazione** – i dati personali e i backup/registri di eventi dovrebbero essere pseudonimizzati come misura di sicurezza per ridurre al minimo i rischi di potenziali violazioni dei dati, ad esempio utilizzando l'hashing o la cifratura;
- backup/registri di eventi – conservare backup e registri di eventi nella misura necessaria per la sicurezza delle informazioni, utilizzare registri delle attività (audit trails) e il monitoraggio degli eventi come controlli di sicurezza su base routinaria, proteggendoli da modifiche e accessi non autorizzati e accidentali e rivedendoli periodicamente, oltre a gestire in modo tempestivo eventuali incidenti;

Art. 25 e principio riservatezza

elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, possono figurare:

- ripristino in caso di disastro (**disaster recovery)/continuità operativa** – soddisfare i requisiti per il ripristino del sistema informativo in caso di disastro e per la continuità operativa, al fine di ripristinare la disponibilità dei dati personali a seguito di incidenti rilevanti;
- protezione in base al rischio – tutte le categorie di dati personali dovrebbero essere protette con misure adeguate contro il rischio di violazioni della sicurezza. I dati che comportano rischi particolari dovrebbero, ove possibile, essere tenuti separati dagli altri dati personali;
- gestione della risposta in caso di incidenti legati alla sicurezza – occorre disporre di metodologie, procedure e risorse per rilevare, limitare, gestire e segnalare le violazioni dei dati e trarne insegnamenti;
- **gestione degli incidenti** – al fine di rendere più solido il sistema di trattamento, il titolare deve disporre di procedure per gestire violazioni e incidenti, ivi comprese procedure di notifica quali la gestione delle notifiche (per l'autorità di controllo) e delle informazioni (per gli interessati).

Provvedimento

illiceità del trattamento - raccolta periodica e automatica di dati personali sanitari (sia pure indirettamente identificativi) riferiti ai pazienti che presso le strutture sanitarie usufruiscono delle apparecchiature diagnostiche per le quali essa fornisce servizi di manutenzione e di assistenza, al loro trasferimento anche verso gli Stati Uniti, nonché all'utilizzo dei medesimi dati per scopi ulteriori

Provvedimento

adottare le misure e gli accorgimenti atti a non consentire con mezzi ragionevoli la re-identificazione dei pazienti interessati, neanche mediante il ricorso ad altre informazioni nella disponibilità della stessa società, di altre società del Gruppo o di terzi

- "*anonimizzare*" efficacemente il flusso sistematico di dati - esempio, alla previsione di valori discreti degli attributi in luogo di valori continui, o di intervalli di valori al posto dei valori puntuali, o ancora all'introduzione, ove possibile, di valori binari, quali vero/falso, al posto di attributi a valori multipli, che garantiscano la raccolta delle sole informazioni le cui combinazioni di valori degli attributi siano riferibili ad un numero di interessati pari o superiore a tre unità. A tal fine, si potrà procedere mediante la ridefinizione del numero di combinazioni di valori possibili degli attributi oggetto di trasferimento in modo tale da assicurare che nei dati ricevuti periodicamente dalla società non ci siano posizioni di pazienti che presentino combinazioni di valori degli attributi in numero inferiore alle tre unità, scartando pertanto quelle posizioni legate a combinazioni rare di valori di attributi che siano riferite a meno di tre pazienti.

Provvedimento

qualora invece per specifici interventi tecnici posti in essere in loco e/o in remoto nell'ambito delle ordinarie attività di manutenzione e di assistenza delle apparecchiature in uso presso le strutture sanitarie, si renda indispensabile il trattamento di dati attinenti alla salute di pazienti (sia pure indirettamente identificativi) per garantire il corretto funzionamento delle stesse, prescrive alla medesima società di adottare le misure opportune

- informare tempestivamente la struttura sanitaria presso la quale viene eseguito dell'intervento tecnico posto in essere anche da remoto;
- documentare alla predetta struttura sanitaria, anche nell'ambito del rapporto tecnico di servizio previsto dal contratto stipulato con quest'ultima, le operazioni di trattamento (effettuate per eseguire l'intervento in loco o in remoto), che hanno avuto ad oggetto dati personali attinenti alla salute dei pazienti (anche qualora riguardino dati indirettamente identificativi), indicando le tipologie di dati coinvolti e le ragioni che hanno reso necessario trattare tali informazioni per assicurare e/o ripristinare il funzionamento dell'apparecchiatura;

Provvedimento

qualora invece per specifici interventi tecnici posti in essere in loco e/o in remoto nell'ambito delle ordinarie attività di manutenzione e di assistenza delle apparecchiature in uso presso le strutture sanitarie, si renda indispensabile il trattamento di dati attinenti alla salute di pazienti (sia pure indirettamente identificativi) per garantire il corretto funzionamento delle stesse, prescrive alla medesima società di adottare le misure opportune

- registrare le predette operazioni di trattamento (*access log*) con modalità tali da assicurarne la completezza, l'inalterabilità e la possibilità di verifica della loro integrità e metterle a disposizione della struttura sanitaria, su richiesta, avendo cura che tali registrazioni comprendano i riferimenti temporali e la descrizione dell'evento che le ha generate e siano conservate per un congruo periodo, non inferiore a sei mesi;
- perfezionare le tecniche di pseudonimizzazione utilizzate in modo da ridurre il rischio di re-identificare gli interessati tramite la disponibilità dell'informazione relativa all'istante di tempo in cui uno specifico evento (ad es. esame diagnostico) è stato generato, adottando sistemi di riordino casuale degli eventi (*shuffling*), ovvero tecniche crittografiche basate sull'applicazione di chiavi variabili nel tempo anche mediante l'utilizzo, all'interno della chiave di codifica, di sequenze causali di bit (c.d *salt*) non riconducibili in alcun modo alla data dell'esame, in modo da ridurre il rischio che un soggetto non a conoscenza della suddetta sequenza possa risalire dai codici pseudonimizzati all'identità del paziente;

AIIC 2024 ROMA

Grazie per l’attenzione!

AIIC associazione italiana ingegneri clinici