PROTEZIONE DEI DATI IN AMBITO SANITARIO

CRISTINA DAGA

Milano, 8 luglio 2017

SICUREZZA E PRIVACY IN SANITÀ

La pianificazione e realizzazione di interventi nell'ambito della sicurezza e della privacy nel contesto della sanità digitale richiede almeno la valutazione di tre considerazioni di fondo:

1. Non esiste il concetto di "sicurezza assoluta"

Qualsiasi sistema è vulnerabile. Mettere in sicurezza un sistema significa pianificare un insieme di procedure e strumenti che consentano di ridurre i rischi nella misura possibile o a livelli di accettabilità

2. Sicurezza e privacy: non impedire di fare ma spingere a fare meglio.

Gli interventi in materia di sicurezza e privacy nell'ambito dell'innovazione digitale non costituiscono "limitazioni" a un utilizzo esteso e pervasivo di ICT ma rappresentano azioni di qualificazione e di miglioramento del sistema informativo a fini di maggior tutela di tutti gli stakeholders coinvolti (azienda, professionisti che operano in essa, cittadini)

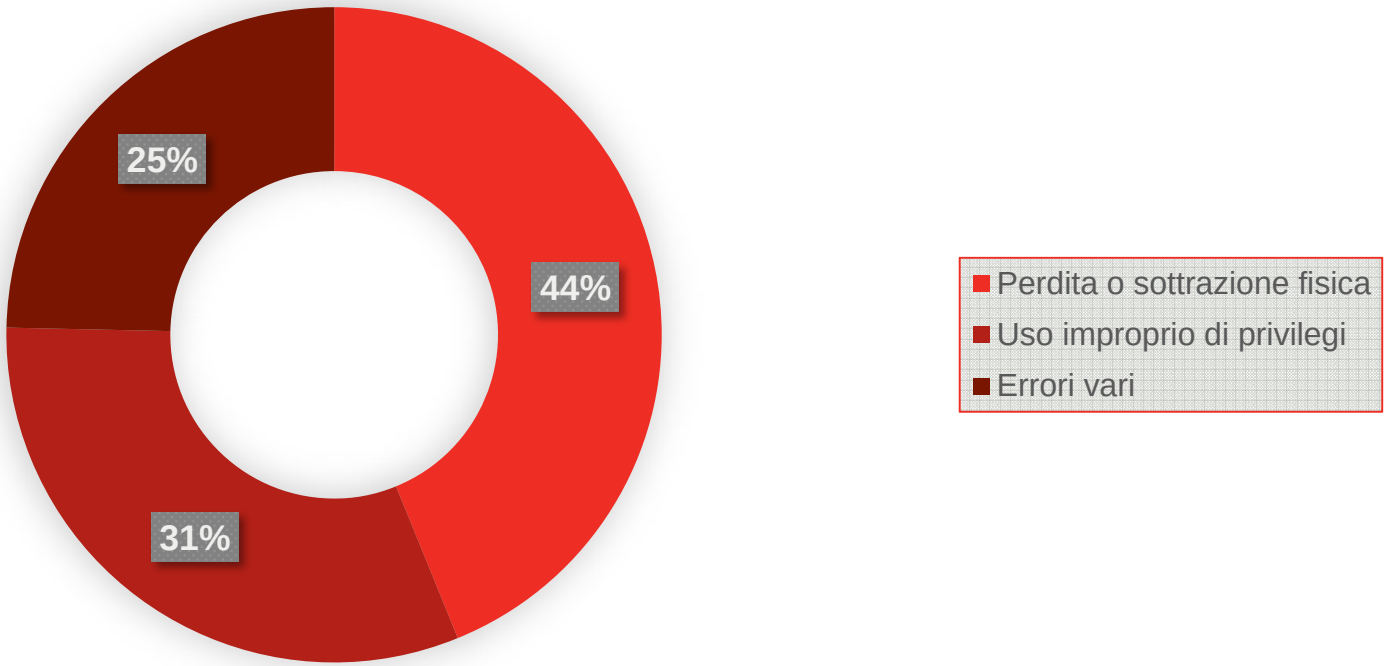
3. Sicurezza e privacy: non solo tecnologia.

Gli interventi nell'ambito della sicurezza e della privacy non si limitano alla sfera tecnologica ma toccano aspetti organizzativi, economici che vanno pianificati e governati nel loro complesso e gli aspetti culturali.

Attacchi nel mondo sanitario

Esistono tre differenti **tipologie di attacco** nel mondo sanitario:

Rappresentano il 73% degli attacchi totali, suddiviso in:



Fonte: Verizon Data Breach Investigation Report

Attacchi nel mondo sanitario: malware

All’interno della Pubblica Amministrazione, la Sanità, è stata quella che ha registrato il maggior numero di attacchi ransomware negli ultimi anni.

COME CONTRASTARLI?

Attraverso lo sviluppo di programmi di sensibilizzazione mirati per gli utilizzatori dei sistemi informativi della PA in aggiunta ad efficaci misure di sicurezza.

AGENZIA DIGITALE ITALIANA

L’AgID ha pubblicato nel 2016 un documento che contiene le “Misure minime di sicurezza ICT per la Pubblica Amministrazione” (parte integrante delle Linee Guida per la Sicurezza).

La normativa privacy in sanità

Regolamento 679/2016 (GDPR)

- Il GDPR pone grande enfasi sulla **sicurezza come obiettivo** da raggiungere. Lo stesso menziona la **cifratura** (come misura di sicurezza) per impedire l'accesso ai dati per i non autorizzati, senza prescrivere quali siano le tecnologie specifiche per gli altri ambiti della sicurezza.
- Vi sono, nell'art. 32 alcune prescrizioni specifiche sulla sicurezza e sull'obbligo di adottare misure tecniche ed organizzative adeguate.
- All'art. 25 si parla di protezione dei dati sin dalla progettazione e per impostazione predefinita (**privacy by design/by default**).
- Tutto il testo muove dal concetto di **accountability** del Titolare (e Responsabile) del trattamento, incrementandone le responsabilità.
- È prevista, inoltre, all'art. 33 una procedura di gestione dei c.d. **Data Breach**, con l'obbligo di notificare all'Autorità Garante (entro 72 ore) una violazione (in casi particolari è previsto l'obbligo di comunicarlo all'interessato – art. 33).

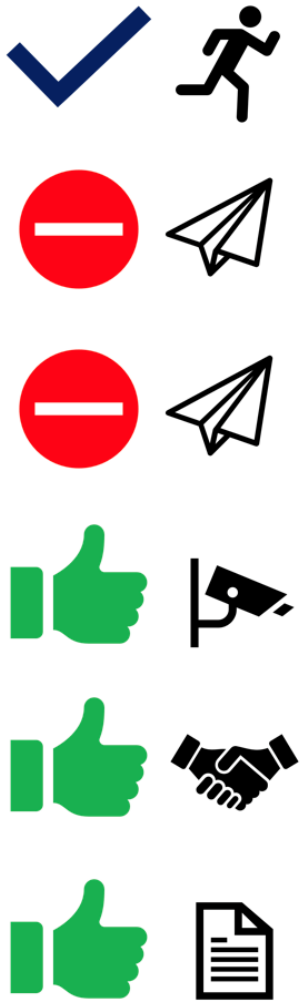
PROVVEDIMENTI GARANTE PRIVACY

- Linee guida in materia di Dossier sanitario – 4 giugno 2015

ORIZZONTE TEMPORALE

COSA ACCADE A MAGGIO 2018

Regolamento 2016/679	**IN VIGORE, NON APPLICABILE (?)**
Direttiva 1995/46	**IN VIGORE, DECADE il 24 maggio 2018**
Autorizzazioni Generali Autorità Garante	**IN VIGORE, DECADONO il 24 maggio 2018**
Provvedimenti Autorità Garante	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Accordi internazionali su trasferimento dati	**NON DECADONO** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissione UE	**NON DECADONO** fino a quando non verranno modificate, sostituite, abrogate



COSA CAMBIA NEL REGOLAMENTO

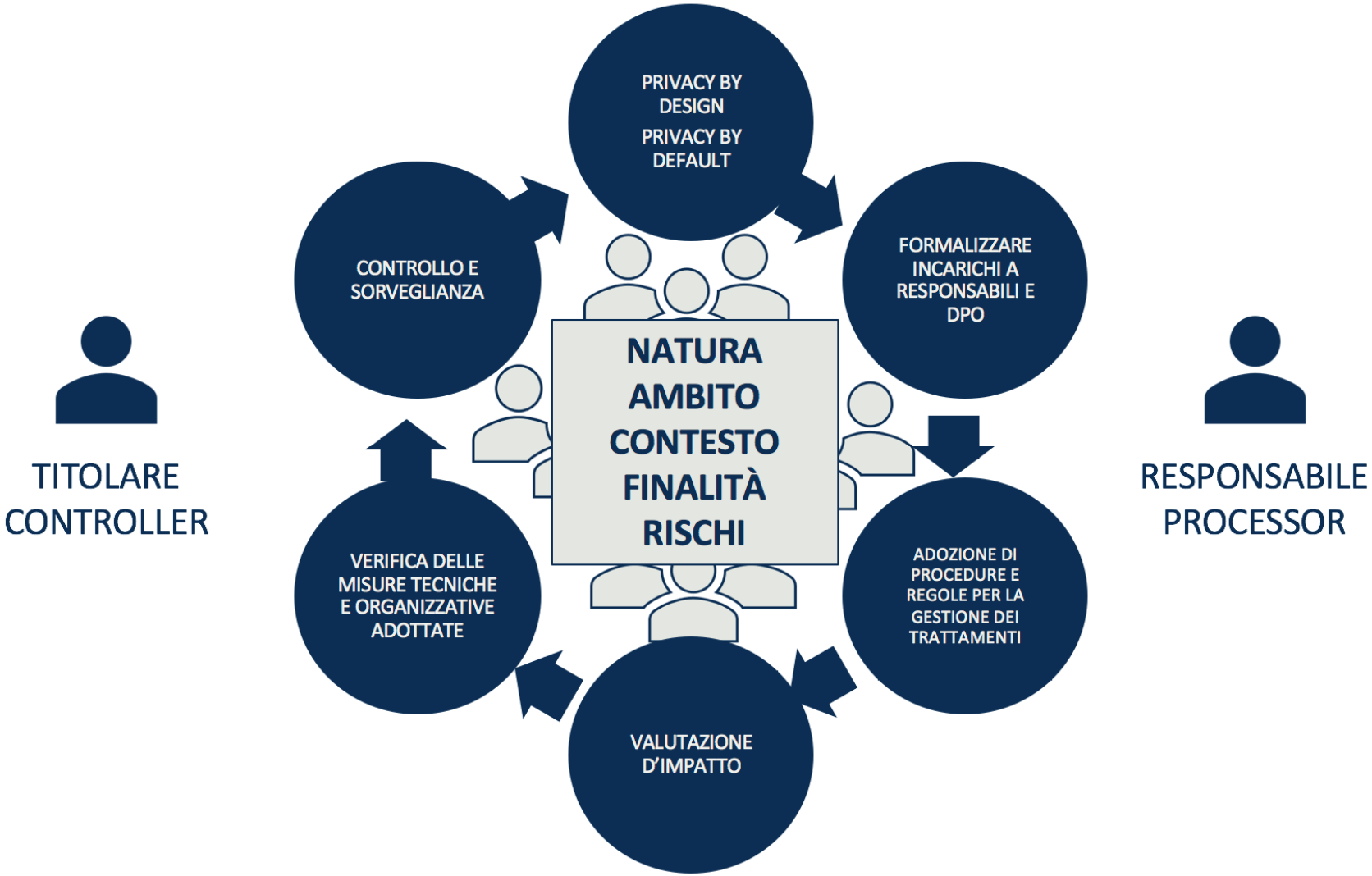
INVARIATI O VARIATI MARGINALMENTE

- Definizione di trattamento
- Definizione di dato personale
- Principi relativi al trattamento di dati
- Liceità del trattamento
- Obbligo di informativa
- Obbligo di consenso
- Soggetti che effettuano il trattamento (salvo incaricati e DPO)
- Protezione delle sole persone fisiche

NOVITA' DEL REGOLAMENTO

- Accountability del titolare
- **Privacy by design**
- Registro dei trattamenti
- **Valutazione dei rischi**
- Adozione di misure tecniche e organizzative adeguate
- Data breach
- Valutazione d'impatto
- **Data Protection Officer (DPO)**
- Certificazione dei trattamenti
- Responsabilità solidale di titolare e responsabile
- Entità delle sanzioni

SISTEMA GESTIONE DATA PROTECTION



VALUTAZIONE DEL RISCHIO

Il trattamento dei dati in ambito sanitario costituisce uno dei contesti più delicati in ragione della natura **“sensibile”** dei dati che attengono allo stato di salute degli interessati, dati rispetto ai quali l’aspettativa di riservatezza e confidenzialità è, tradizionalmente, molto elevata e la legge garantisce i più alti livelli di protezione.

Un criterio importante è senz’altro la "data protection by default and by design" *(si veda art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili ***"al fine di soddisfare i requisiti"*** del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a **monte**, prima di procedere al trattamento dei dati vero e proprio e richiede **un'analisi preventiva e un impegno applicativo** da parte dei titolari che devono sostanziarsi in **una serie di attività specifiche e dimostrabili.**

VALUTAZIONE DEL RISCHIO

Il principio della “privacy by design” si pone l’obiettivo di:

- garantire uno **sviluppo tecnologico** più equilibrato, e
- Incoraggiare **gli sviluppatori di prodotti, servizi e applicazioni a tenere conto del diritto alla protezione dei dati sin dalla fase di progettazione.**

La TUTELA è molto più efficace se gli strumenti (hardware e software) utilizzati per il trattamento dei dati personali sono concepiti, sin dall’origine, **per un uso responsabile dei dati applicando il criterio della minimizzazione e tecniche di pseudonimizzazione degli stessi**, riducendo così i rischi del trattamento e, conseguentemente, l’impatto sui diritti degli interessati.

Inoltre, considerare l’impatto privacy delle tecnologie, sin dalla progettazione, è anche un criterio di efficienza **in quanto evita interventi successivi che potrebbero rallentarne lo sviluppo con conseguenti riflessi negativi in termini di costi.**

Fonte: Modafferi, Garante Privacy

VALUTAZIONE DEL RISCHIO

In questo contesto il legislatore può dare un importante contributo spingendo il **settore pubblico** e, in particolare l'ambito sanitario, a far tesoro dell'indicazione riportata nel considerando n. 78 del Regolamento 2016/679/UE secondo la quale

"i principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici", in modo che la privacy by design diventi un elemento essenziale nella selezione delle forniture di beni o servizi deputati al trattamento dei dati personali per la Pubblica amministrazione e per la Sanità.

Come proteggere i dati: obiettivi

Fonte: Oracle