Iniziativa per la definizione di un codice di condotta per la protezione dei dati personali in sanità

Bozza del codice di condotta

documento fmf-001/0119 versione 0.91 del 22-02-2019

Contributi espressi insieme alla dichiarazione di consenso

Questo documento riassume i contributi forniti dai partecipanti insieme alla dichiarazione di consenso, il cui prospetto riassuntivo è riportato in allegato.
Per alcuni contributi, è aggiunto un commento per facilitare ulteriori approfondimenti e chiarimenti.
I contributi per i quali non viene indicato alcun commento, verranno direttamente integrati nella prossima versione del documento

Iniziativa per la definizione di un codice di condotta per la protezione dei dati personali in sanità

Cap 1. Premessa

a. Completezza

Baratto

1.1. Nelle premesse specificherei meglio la finalità del Codice di Condotta (e un accenno alla differenza con le regole deontologiche) post D.Lgs 101/2018, evidenziando che contiene regole di condotta e criteri, non vincolanti, elaborati da vari organismi (specificare chi ha contribuito alla redazione) ma che l'importanza dell'adesione al Codice di Condotta , approvata dal Garante per la Protezione dei dati personali, risiede nel fatto che può essere utilizzata dal Titolare come elemento di prova di conformità al GDPR, nell'ambito dell'obbligo della prova che lo stesso ha di aver attuato le misure organizzative e di sicurezza adeguate alla particolare tipologia di dati.
Specificherei meglio a quali soggetti è destinato il Codice di Condotta

Commentato [FMF1]: aggiornato

Commentato [FMF2]: aggiornato

Caputo

- Citare sempre servizi sanitari e socio-sanitari
- Non inserire nomi fra " ": si rischia di battezzare concetti spesso non applicabili in alcuni enti

Commentato [FMF3]: aggiornato

Mazzeo

Forse andrebbe maggiormente evidenziato il fatto che il Codice di condotta è volto ad offrire alle strutture sanitarie pubbliche e private di ogni ordine e grado, i criteri guida cui affidare il corretto trattamento di dati personali in quell'ambito.

Commentato [FMF4]: inserito

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Baratto

Non capisco, però, la frase di cui al punto 1.1. lett. b) ….in una forma non ambigua ma al tempo stesso di validità generale…….

Commentato [FMF5]: reso più esplicito

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Cap. 2. Definizioni

a. Completezza

Caputo

Citare alcune esemplificazioni/sinonimi, come nel caso della parola procedura, in alcuni enti chiamata protocollo, linea-guida, istruzione operativa.

Commentato [FMF6]: E' esplicitato che le definizioni hanno rilevanza ai soli fini della terminologia utilizzata nel documento del codice., descrivendo il significato dei termini stessi. Per chiarezza è opportuno mantenere una terminologia uniforme

Vitacca

Può essere opportuno includere, nei trattamenti secondari, l'eventuale trattamento di dati/immagini nell'ambito della videosorveglianza finalizzata alla prevenzione di abusi su ospiti anziani o utenza fragile.
Sono diversi i disegni in questo ambito e non mancano delibere regionali (es. Liguria) che prevedono sistemi di videosorveglianza, nei luoghi di residenzialità. Sarebbe opportuno, al riguardo, un invito al Garante a prendere posizione e dare indicazioni chiare a chi, sia a livello nazionale sia a livello regionale ha il potere di legiferare in materia, al fine di prevenire situazioni di confusione normativa simile a quanto già avvenuto in tema di fatturazione elettronica.

Commentato [FMF7]: **Da approfondire nelle versioni successive del codice**

Mazzeo

Persona autorizzata – Anonimizzazione

Commentato [FMF8]: inserito

b. Correttezza

Baratto

2.DEFINIZIONI e 3.1 TIPOLOGIE di DATI TRATTATI

Dati PERSONALI (: preciserei che ...sono tutti i dati personali, riferiti a persone fisiche, ..identificate o identificabili che includono , dati genetici, biometrici e dati relativi alla salute , come definiti nell'art. 4 punto 15 del GDPR, nonché dati relativi a condanne penali e reati (art. 10 GDPR)

3.1.1 toglierei dopo "dati relativi alla salute" e dati idonei a rivelare lo stato di salute (perché non sono un'ulteriore categoria) edi considerando (35)

3.1.2 DECEDUTI : propongo di rivedere/approfondire il trattamento dei dati dei deceduti sia in termini di modalità di trattamento che relativamente all'esercizio dei diritti da parte di chi ha un interesse proprio, o agisce a tutela dell'interessato deceduto , in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione prevista espressamente dal legislatore italiano con il D.lgs 101/2018. DEDICHEREI UNA SEZIONE APPOSITA (3.1.2.3)

3.2.4 Trattamenti finalizzati ad analisi a supporto di decisioni del titolare in merito alla propria attività. Poiché sono dati anonimi e quindi non si applica il GDPR porterei, per maggior chiarezza, la nota 6 direttamente sotto a questo punto anziché al punto 3.2.4.2

3.2.5 Trattamenti finalizzati alla ricerca in campo medico biomedico e epidemiologico e ricerca scientifica

3.2.5 .1 Le attività di ricerca in campo medico (*aggiungerei)* biomedico , epidemiologico e scientifico possono articolarsi secondo due scenari

Caputo

Il concetto di nucleo di riferimento andrebbe chiarito in rapporto ai ruoli previsti dal GDPR

Iacono

La definizione di "Sistema di gestione" non è chiara. In realtà è un modello organizzativo come descritto sotto – solo come indicazione:

"I sistemi di gestione aziendali sono modelli organizzativi aziendali adottati su base volontaria e realizzati mediante l'applicazione organica e sistematica di regole e procedure che una azienda fa proprie a tutti i livelli dell'organizzazione allo scopo di raggiungere uno specifico obiettivo. Un sistema di gestione aziendale si realizza condividendo alcuni semplici principi: • dire quello che si vuole fare • fare quello che si è detto, • registrare quello che è accaduto per poter controllare e dare evidenza documentale di quello che si è fatto • trarre insegnamento dai propri errori e cercare continuamente di migliorare ciò che si è fatto"
(Fonte http://www.safetymanagementsite.it/index.php?option=com_content&view=article&id=95&Itemid=538)

Commentato [FMF9]: il codice è circoscritto allo scenario dei dati personali

Commentato [FMF10]: aggiornato

Commentato [FMF11]: verrà dettagliato in versioni successive

Commentato [FMF12]: alcuni trattamenti, in questa tipologia, prevedono anche l'uso di dati non anonimi

Commentato [FMF13]: aggiornato. I trattamenti epidemiologici sono una tipologia separata

Commentato [FMF14]: nella definizione si fa riferimento solo al ruolo professionale rispetto all'erogazione dei servizi. Le eventuali relazioni con i ruoli individuati dal GDPR (titolare, etc.) -se necessario- saranno approfonditi nei § successivi

Commentato [FMF15]: aggiornato

Sammartino

1) A MIO PARERE, ALLA VOCE "DATI PERSONALI" SI DOVREBBE FAR RIFERIMENTO ANCHE AI DATI "PARTICOLARI" CHE COMPRENDONO I DATI GENETICI, I DATI BIOMETRICI E QUELLI SULLA RELIGIONE. NON BISOGNA DIMENTICARE, INFATTI, CHE IN TUTTI GLI OSPEDALI, VENGONO TRATTATI DATI SULLA RELIGIONE PER L'ASSISTENZA SPIRITUALE DEI PAZIENTI CHE NE FANNO RICHIESTA.
2) AL POSTO DI "MASCHERAMENTO" METTEREI "ANONIMIZZAZIONE", IN QUANTO LA DEFINIZIONE CHE NE VIENE DATA SEMBRA RIFERIRSI PIU' ALLA RIMOZIONE DEFINITIVA DEI DAI RIFERITI AL PAZIENTE CHE DI UNA CODIFICA.

Commentato [FMF16]: aggiornato

Commentato [FMF17]: è stato specificato che il mascheramento conserva informazioni rilevanti dal punto di vista statistico, pur non consentendo l'individuazione della persona

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Mazzeo

Forse andrebbe preferito un linguaggio meno tecnico a favore di una maggiore comprensibilità generale dei testi

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

E' opportuno definire più in dettaglio le caratteristiche del "percorso" con le conseguenti esigenze di collaborazione e condivisione

Cap. 3. Tipologie di dati, trattamenti e finalità

a. Completezza

Vitacca

Nella individuazione della liceità dei trattamenti finalizzati all'erogazione dei servizi sanitari, sociosanitari e socio-assistenziali (par. 3.2.2.3 e seguenti) potrebbe essere opportuno prevedere il caso delle attività socio-assistenziale a favore di soggetti AUTOSUFFICIENTI.

Commentato [FMF18]: **da approfondire sotto il profilo giuridico**

Anche se il codice privacy prevede il solo caso di soggetti minori, bisognosi, non autosufficienti e incapaci (art. 2-sexies par. 2 lett s), non sono pochi i casi in cui strutture residenziali offrono servizi a favore di utenza ancora autosufficiente.

Con riferimento alla liceità dei trattamenti finalizzati all'erogazione dei servizi sanitari, sociosanitari e socio-assistenziali (par. 3.2.2.3 e seguenti) sarebbe opportuno dare delle indicazioni per quanto riguarda il riferimento all'art. 9 par. 3 del Regolamento laddove si parla di "altra persona anch'essa soggetta all'obbligo di segretezza"
La formulazione del Regolamento distingue tra obbligo di chi è soggetto a segreto professionale e quello di "altra persona anch'essa soggetta all'obbligo di segretezza", riservato quindi a figure non sanitarie (es. amministrativi che operano in accettazione, controllo di gestione ecc.).
Il Regolamento fa riferimento all'obbligo di segretezza in conformità al diritto dell'Unione/ Stato membro o norme stabilite da "organismi nazionali competenti". Trattandosi di obbligo diverso dal segreto professionale (regolato da codici deontologici), il codice di condotta può fungere da "norma stabilita da organismo competente" o l'unico riferimento possibile è una regolamentazione aziendale interna?

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Cap. 4. Sistema per la protezione dei dati personali

4.1 Struttura organizzativa

a. Completezza

Baratto

Non metterei come definizione blindata "Comitato per la Protezione dei dati personali" ma lascerei più libertà alle organizzazioni di definire la propria struttura organizzativa (es. Gruppo Privacy, o Board/DPO aziendale o Gruppo di lavoro in materia di protezione dei dati personali etc.)

Caputo

Evitiamo di battezzare nomi con impatto organizzativo. Il Comitato potrebbe avere nomi quali DPO-team, Gruppo di lavoro, o Tavolo.
Anche la parola Manuale, va modificata e non messa fra " ".

Ferrari

Condivido la necessità che ci si doti di una struttura organizzativa con ruoli chiaramente definiti, ma per rendere l'approccio massimamente estensibile al contesto di riferimento, rivaluterei l'idea del "Comitato per la protezione dei dati personali".
Forse potrebbe risultare più agevole declinare l'istituzione di un "Ufficio per la protezione dei dati personali" istituito a cura del Titolare, da rappresentare all'interno dell'organigramma privacy aziendale, in staff al Titolare medesimo.
Inoltre, nell'ambito di tale struttura nella quale l'RPD svolgerà ruolo essenziale di coordinamento e supporto al Titolare, oltre alle tre categorie di referenti indicate nei punti a), b), c), ed i Responsabili del trattamento, risulterà altresì opportuna l'aggiunta dell'Organismo di Vigilanza ex. D.lgs. 231/2001(OdV), magari anche in funzione di Organismo indipendente di Valutazione (OiV), come stabilito dalle recenti disposizioni ANAC (Delibera n°141 del 21/02/2018), stante gli obblighi di pubblicazione e trasparenza, nonché l'accesso civico discendente, posto in capo agli enti di diritto privato, analogamente a quanto già avviene per la Pubblica Amministrazione.
In una logica di "*compliance*" aziendali integrate, la funzione dell'OdV non può non vedersi interconnessa con quella dell'RPD. Entrambe le figure, supportano il Titolare nella valutazione del rischio, ciascuna per la propria competenza ed il proprio ruolo legale, ma in una prospettiva moderna di adesione ad un codice di condotta, devono anche iniziare a dialogare in una "sede" comune di confronto e di scambio reciproco. Il confronto, potrebbe/dovrebbe estendersi anche all'RSPP, altra figura "consulente" del Titolare in materia di valutazione del rischio.
Da ultimo per quelle strutture che si sono dotate di un sistema interno di gestione di risk management o processo di gestione del rischio, inteso come "*l'insieme di attività, metodologie e risorse coordinate per guidare e tenere sotto controllo un'organizzazione con riferimento ai rischi*", l'Ufficio/Comitato da cui si è partiti, potrebbe caratterizzarsi per la presenza di tutti i ruoli richiamati, nella loro funzione in staff al Titolare.

Mazzeo

Commentato [FMF19]: aggiornato

Commentato [FMF20]: aggiornato

Commentato [FMF21]: tolte le " "; per coerenza e leggibilità il documento deve comunque basarsii su una terminologia omogenea

Commentato [FMF22]: aggiornato. E' specificato che questo "comitato" viene istituito dal titolare con il nome e nelle forme più opportune alla specifica organizzazione, fermo restando l'obiettivo ed i compiti

Commentato [FMF23]: E' prevista la possibilità di ulteriori apporti derivanti dallo specifico contesto di attività del titolare

A mio parere si mortifica troppo il ruolo del DPO che, viceversa, risulta centrale nel nuovo impianto del GDPR. A prescindere dalla sua presenza nel Comitato, il DPO non viene praticamente più citato nel documento, attribuendo al Comitato quelli che sono anche compiti propri – ed esclusivi – del DPO per espressa disposizione di norma.

Orsini-Perciballi

In merito al Comitato non si evince chiaramente da chi è costituito, si parla genericamente del fatto che il comitato si avvale "di referenti dell'organizzazione almeno relativamente alle seguenti aree.. a, b, c" ma non si comprende se detti referenti sono componenti del comitato stesso o consulenti esterni al comitato.
Nel caso in cui si tratti di componenti del comitato si suggerisce di valutare la possibilità di far esprimere i membri dello stesso dai Dipartimenti in modo da avere la maggior omogeneità professionale all'interno dell'azienda.

Secondo capoverso aggiungeremmo tra parentesi (…, tecnici, ..)

b. Correttezza

Boscariol

non sono convinto della necessità di rendere obbligatorio un Comitato per la protezione dei dati, perlomeno non in tutte le situazioni.
Non sono convinto che sia necessario per ogni normativa e per ogni struttura creare un Comitato che oramai cominciano ad essere molti nelle strutture sanitarie e socio-sanitarie, con le relative criticità organizzative

Iacono

Responsabilità della Direzione – Non si capisce bene chi è la Direzione (Direzione Sanitaria – Amministrativa – Ecc.)
ERRORE "effettati" invece di "effettuati"

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli

Commentato [FMF24]: Il ruolo e le attività del DPO saranno oggetto di un appositi capitolo aggiuntivo del codice, attualmente in fase di elaborazione da parte di un gruppo di lavoro designato, anche alla luce dei criteri organizzativi e tecnologici generali definiti ìn questa versione.
Per questo motivo questo aspetto non è stato approfondito nella versione attuale

Commentato [FFM25]: Il codice propone la istituzione di questo "comitato" per assicurare una visione più organica delle diverse esigenze e prospettive di rischio. La struttura e la forma organizzativa (come indicato nella nota a piè di pagina) è lasciata alle singole strutture, in funzione delle loro caratteristiche e dimensioni.

Commentato [FMF26]: E' specificato che questo "comitato" viene istituito dal titolare con il nome e nelle forme più opportune alla specifica organizzazione, fermo restando l'obiettivo ed i compiti.

Commentato [FMF27]: Aggiornato: è specificata "Direzione aziendale", applicabile quindi in tutti i contesti organizzativi,

L'adeguamento avverrà in modo graduale per via dei numerosi interventi necessari e soprattutto per il cambiamento di mentalità necessario rispetto alla concezione attuale di privacy

Sammartino

HO DELLE FORTI RISERVE SUL FATTO CHE IL COMITATO PER LA PROTEZIONE DEI DATI PERSONALI – AL DI FUORI DEL DPO – SIA IN GRADO DI ASSOLVERE AI COMPITI CHE GLI VENGONO ASSEGNATI.

Mazzeo

Mi sembra che si viaggi verso un'eccessiva burocratizzazione dell'organizzazione che, viceversa, dovrebbe essere principalmente un presidio "snello" di ausilio al Titolare in collaborazione con il DPO

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

4.2 Documentazione di riferimento

a. Completezza

Caputo

Non inserire nomi fra " ": si rischia di battezzare concetti spesso non applicabili in alcuni enti

Ferrari

Ridondante la richiesta di giungere attraverso il Comitato per la protezione dei dati personali, ad un "Manuale di riferimento per la protezione dei dati personali".
Peraltro, tale onere strettamente non si ha neppure nell'ambito dei sistemi di certificazione ISO 27001:2014 ove i punti fermi sono dati da: monitoraggio, misurazione, analisi e valutazione, audit interni, riesame della direzione, azioni di miglioramento.
Maggiormente funzionale al principio di accountability (privacy by design, privacy), ed alla DPIA, l'introduzione/adozione di una metodologia di mappatura delle aree di trattamento dell'organizzazione, che permetta di ricostruire le procedure organizzative e di formazione definite dal Titolare e/o dai Responsabili, fino a giungere ad una vera e propria policy privacy aziendale.

Sammartino

Commentato [FMF28]: E' stato specificato che-ai fini del codice- il "comitato" rappresenta l'impegno ad una collaborazione fra i referenti delle diverse aree di interesse all'interno dell'organizzazione, e che viene attualizzato dal titolare nelle forme e nei modi più consoni con la struttura organizzativa

Commentato [FMF29]: E' stato specificato che-ai fini del codice- il "comitato" rappresenta l'impegno ad una collaborazione fra i referenti delle diverse aree di interesse all'interno dell'organizzazione, e che viene attualizzato dal titolare nelle forme e nei modi più consoni con la struttura organizzativa

Commentato [FMF30]: Aggiornato, in ogni caso il contenuto e gli obiettivi dei documenti è definito per ognuno di essi

Commentato [FMF31]: E' stato sottolineato che "manuale" rappresenta un documento di riferimento complessivo avente lo scopo di assicurare l'organicità e la reperibilità dei documenti

Commentato [FMF32]: Per quanto riguarda le attività informatizzate, è previsto il registro dei sistemi informatizzati.
La definizione di una metodologia di analisi dei processi nell'ottica della protezione dei dati personali è al di fuori degli scopi del codice. Se proposta potrebbe costituire un allegato o un documento complementare

ALLA SECONDA RIGA DEL PARAGRAFO 4.2 SI FA RIFERIMENTO ALL'ORGANIZZAZIONE PER LA PROTEZIONE DEI DATI DI CUI, PERO', SALVO UNA MIA SVISTA, NON HO TROVATO ALCUNA DEFINIZIONE PREGRESSA.

Commentato [FMF33]: Formulato in modo più chiaro

Mazzeo

Inventario delle possibili violazioni di dati personali/dei data breach concretizzati. A fronte di un numero rilevante di documenti – che magari potrebbero essere ridotti e riaccorpati – ritengo manchi un registro data breach la cui necessaria adozione si rinviene nelle norme del GDPR

Commentato [FMF34]: Aggiunto l'inventario delle violazioni (e la definizione)

b. Correttezza

Baratto

Non metterei la definizione di "Manuale per la protezione dei dati personali" ma lascerei all'organizzazione la decisione di denominare il proprio documento "regolatorio" interno (es. Regolamento per la protezione dei dati personali etc.)

Commentato [FMF35]: E' esplicitato che le definizioni hanno rilevanza ai soli fini della terminologia utilizzata nel documento del codice., descrivendo il significato dei termini stessi. Per chiarezza è opportuno mantenere una terminologia uniforme

c. Valutazione e osservazioni in termini di usabilità

Mazzeo

Ha un rischio di eccessiva burocratizzazione dei processi

Commentato [FMF36]: Considerata l'articolazione delle problematiche e delle responsabilità (anche in termini di accountability) o documenti individuati definiscono un contesto minimo ma organico mediante il quale poter gestire i vari aspetti e rispondere agli obblighi di accountability.
La forma di registrazione e di tenuta dei documenti è lasciata alla decisione dei titolare, ferme restando le esigenze di reperibilità, tracciabilità.

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli

Sui dispositivi medici trovo poco applicabile la gestione di un database che venga tenuto costantemente aggiornato ma ne condivido l'importanza

Commentato [FMF37]: Per quelli collegati in rete è anche un obbligo prescritto dalle misure AgID

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

In assenza di uno specifico SW si dovrebbe indicare la possibilità di soluzioni informatiche per avere il registro dei sistemi informatizzati e il registro dei profili di abilitazione in modo aggiornato continuamente

Commentato [FMF38]: Aggiunto una nota a questo proposito

4.4 Verifiche periodiche

a. Completezza

Falcini

Chiarire il rapporto fra Audit del comitato e valutazioni del DPO

Commentato [FMF39]: Esplicitato che il risultato degli audit è oggetto di esplicite valutazioni da parte del DPO

Ferrari

Potrebbe essere utile giungere a definire item di verifica degli audit

Commentato [FMF40]: La definizione di istruzioni operative che propongano il dettaglio dell'attuazione di questo e di altri aspetti

Mazzeo

Manca una codifica del ruolo del DPO negli audit che, quantomeno per quelli interni, a mio parere dovrebbe essere protagonista

Commentato [FMF41]: Cfr commento precedente sul ruolo complessivo del DPO, oggetto di una apposita sezione del codice in fase di elavorazione

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli

Nelle Aziende di grandi dimensioni trovo difficile organizzare audit periodici per verificare l'applicazione del GDPR mentre troverei più fattibile indicare l'opportunità di visite periodiche nelle UU.OO. del DPO

Commentato [FMF42]: L'organizzazione delle verifiche, in termini di responsabili, aree e contenuti è definito dall'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Caputo

Check-list per verifiche periodiche

Commentato [FMF43]: **Da approfondire, insieme ad altri template e best-practices in versioni successive del documento**

Ferrara

Sarebbero opportuni dei template

Commentato [FMF44]: **Cfr commento precedente**

4.5 Formazione

a. Completezza

Baratto

Il titolare definisce procedure al fine di assicurare una adeguata formazione, ed essere in grado di dimostrarla, sui principi del Regolamento….. …..La formazione comprende sia una fase iniziale, al momento dell'inizio della collaborazione, sia momenti periodi di verifica ed aggiornamento definiti secondo un piano annuale.

Si potrebbe specificare che la formazione può avvenire anche con FAD

Commentato [FMF45]: Specificato che la formazione si basa su metodologie e tecnologie stabilite dal titolare

Mazzeo

Anche in questo caso direi che manca il ruolo del DPO che, a mio parere, dovrebbe essere protagonista assoluto della formazione interna avendo fra i suoi compiti principali proprio l'educazione alla compliance

Commentato [FMF46]: Cfr quanto evidenziato sul ruolo del DPO

Orsini-Perciballi

Si suggerisce di affidare la definizione delle procedure di formazione ed aggiornamento del personale al Comitato per la protezione dei dati personali o al più ad entrambi. In seno a questo comitato infatti sono ben rappresentate le aree su cui insiste il personale coinvolto nel trattamento dei dati.

L'eventuale accoglimento della modifica va poi riportata anche al secondo capoverso.

Commentato [FFM47]: riportato

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Sarebbe opportuno qualche riferimento sulle varie aree di formazione

Commentato [FMF48]: Da indicare in evoluzioni successive

4.3 Monitoraggio

a. Completezza

Ravaioli

LO TROVO UNA RIPETIZIONE DEL CAPITOLO 4.3 COME CONTENUTO

Ravaioli

Come nei casi precedenti, manca l'evidenza del necessario ruolo del DPO

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

Pare un po' generico; può essere collegato al punto 4.3

Ferrara

Sarebbero opportuni riferimenti e template sulle modalità possibili

4.6 Rapporti con i responsabili del trattamento

a. Completezza

Ferrara

Vanno definiti meglio i criteri secondo cui si definiscono i ruoli

Commentato [FMF49]: E' stato precisato che, a differenza degli audit (periodici), il monitoraggio riguarda un'attività continua di verifica di componenti (processi e sistemi) specifici. E che risultati del monitoraggio rappresentano un elemento di rilevanza ai fini degli audit. Per coerenza, il paragrafo è stato quindi spostato (come § 4.2), prima di quello relativo alle verifiche periodiche (rinominato 4.3)

Commentato [FMF50]: Cfr punto precedente

Commentato [FMF51]: Da indicare in evoluzioni successive

Commentato [FMF52]: Da indicare in evoluzioni successive

b. Correttezza

Mazzeo

Forse andrebbero specificati dei requisiti base necessari per ogni responsabile del trattamento

Commentato [FMF53]: Da approfondire già nella prima versione

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Squillace

Individuare il Responsabile in ambito sanitario è tema di grande discussione. Se e quando arriveremo ad uno schema, che per quanto poco specifico potrà essere applicato da tutte le strutture sanitarie, e comunque per dare continuità anche alla presenza espositiva del documento, sarebbe opportuno implementare questa sezione.

Commentato [FMF54]: Questa tematica è oggetto degli approfondimenti in corso

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Vanno definiti meglio i criteri secondo cui si definiscono i ruoli

Commentato [FMF55]: Da approfondire già nella prima versione

Cap. 5. Rapporti con l'interessato

5.1 Informativa

a. Completezza

Ferrara

Andrebbero riportati in dettaglio i vari aspetti da citare, menzionati in altre parti del documento

Commentato [FMF56]: Da approfondire già nella prima versione

Orsini - Perciballi

Nell'ultimo capoverso del 5.1.1 si suggerisce di eliminare la parte relativa alle attività di identificazione dell'interessato finalizzate alla promozione di nuovi servizi dato che si possono utilizzare altre forme di comunicazione ed informazione.

Commentato [FFM57]: Trattandosi di profilazione è necessario esplicitare che viene effettuata su dati pseudonimizzati, e -di conseguenza- la finalità di eventuali identificazioni

Nel 5.1.2 lettera b) meglio parlare di relazioni amministrative con gli utenti ed eliminare la parola pazienti che circoscrive l'ambito ad una sola fattispecie.

Commentato [FFM58]: riportato

b. Correttezza

Baratto

5.1.1 Da approfondire la PROFILAZIONE (ove prevista) poichè l'art. 22, par. 4, del GDPR vieta, come principio generale, la profilazione dei dati sanitari, anche se con alcune eccezioni.

Commentato [FMF59]: Nell'informativa è evidenziato che tutti i trattamenti che comportano la profilazione operano su dati psudonimizzati e che l'identificazione della persona avviene -secondo procedure registrate- solo nel caso si riscontrano situazioni di interesse (rischio) per la persona stessa

Sammartino

NEL 3° E NEL 4° CAPOVERSO SI FA RIFERIMENTO ALLA PROFILAZIONE. E' PROPRIO COSI' ? TENUTO CONTO DELLO SCOPO PER CUI VERREBBE SVOLTA QUESTA ATTIVITA' NON SAREBBE FORSE MEGLIO PARLARE DI "SEGMENTAZIONE"?

Commentato [FMF60]: Cfr punto precedente

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

5.2 Consenso

Commentato [FMF61]: **Tutto l'argomento del consenso (§ 5.2) sarà dettagliato ed aggiornato in base ai pronunciamenti del Garante ed al contenuto delle previste misure di garanzia, già prima della finalizzazione della prima versione del codice**

a. Completezza

Baratto

Sul tema del consenso ho numerosi dubbi e auspico, quanto prima, il Provvedimento di chiarimenti del Garante

5.2 Il consenso dell'interessato acquisto, è acquisito…….e si intende valido a tempo indeterminato..

5.2.1 a) ..psudonomizzatipseudonimizzati……..FIDELIZZAZIONE (ove prevista) non mi risulta che le Aziende sanitarie effettuino fidelizzazione DA APPROFONDIRE. - b) da valutare in rapporto al DSE e FSE

Caputo

Numerosi dubbi: esca quanto prima la comunicazione di chiarimento del Garante

Ferrara

Andrebbero riportati in dettaglio i vari aspetti da citare, menzionati in altre parti del documento

Mazzeo

Non concordo sull'assioma che il MMG possa conoscere senza consenso dell'interessato i dati rilevati nel Nucleo. In realtà il paziente deve poter dire che NON vuole che il MMG conosca le informazioni mediche che lo riguardano

Sammartino

- MANCA LA PREVISIONE DEL CONSENSO PER I PROGETTI DI RICERCA

Vitacca

- Raccolta di consenso per accesso al dossier sanitario o a documentazione relativa ad eventi clinici pregressi, fintanto che il Garante non disponga diversamente nell'ambito delle misure di garanzia da adottarsi sulla base dell'art. 2-septies del Codice
  Linee guida dossier sanitario 4 giugno 2015: Il trattamento dei dati sanitari effettuato tramite il dossier costituisce, pertanto, un trattamento ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico per il quale l'interessato si rivolge ad esso…..costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo. All'interessato, infatti, deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un dossier sanitario, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale strumento. Ciò significa che qualora l'interessato non manifesti il proprio consenso al trattamento dei dati personali mediante il dossier sanitario, il professionista che lo prende in cura avrà a disposizioni solo le informazioni rese in quel momento dallo stesso interessato (ad es., raccolta dell'anamnesi e delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista.
  Art. 22 d. lgs. 101/18 comma 4): A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto.
  Anche il recentissimo provvedimento del Garante (nr. 55 del 7 marzo 2019), conferma che attualmente resta confermato il consenso. Tuttavia, come specificato dal Garante stesso in tale provvedimento "**sarà il Garante ad individuare, nell'ambito delle misure di**

garanzia da adottarsi sulla base dell'art. 2-septies del Codice, i trattamenti che, ai sensi dell'art. 9, par. 2, lett. h), possono essere effettuati senza il consenso dell'interessato".

- Può essere opportuno prevedere se e quando è possibile **non raccogliere il consenso** per la raccolta di dati di contatto (es. indirizzo email, cellulare) in sede di accettazione per l'invio successivo di informazione sui servizi offerti a condizione che non costituisca mera finalità promozionale o commerciale.
  L'art. 130 comma 4) d. lgs. 196/03 modificato dal d. lgs. 101/18 prevede la non necessità del consenso (ma della sola informazione) in caso di utilizzo de dati di contatto raccolti in sede di accettazione, per comunicazione in merito ai servizi offerti dal titolare. Infatti il comma 4) prevede: "Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, e' informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.
  Nel caso in cui, tuttavia, la newsletter o la comunicazione via sms costituisca mera attività promozionale o commerciale, sarebbe comunque necessario il consenso (rif. provvedimento del Garante n. 55 del 7/3/2019)

Orsini - Perciballi

Il consenso non può essere acquisito a tempo indeterminato ma deve essere finalizzato al singolo trattamento e deve prevedere la possibilità di scelta e di
revoca dell'interessato per ogni singolo trattamento.

Punto 5.2.2 Modalità di acquisizione del consenso suggeriamo di aggiungere un'ulteriore punto
f) "il consenso informato, acquisito nei modi e con gli strumenti più consoni alle condizioni del paziente, è documentato in forma scritta o attraverso videoregistrazioni o, per la persona con disabilità, attraverso dispositivi che le consentano di comunicare. Il consenso informato, in qualunque forma espresso, è inserito nella cartella clinica e nel fascicolo sanitario elettronico".

Nel punto b) stesso sotto-paragrafo suggeriamo di prevedere tutte le modalità di sottoscrizione elettronica previste dal nuovo CAD .
Nel punto e) specificare anche la modalità analogica Raccomandata A/R e modalità con posta elettronica ordinaria allegando quindi anche il documento di identità

Pagarafo 5.2.3 si ricorda quanto sopra in merito alla non possibilità di acquisire un consenso a tempo indeterminato è bene inoltre specificare che in caso di separazione o divorzio con affido condiviso è necessario il consenso di entrambi i genitori.

b. Correttezza

Ferrara

Verificare l'applicabilità del documento scansionato

Sammartino

- IL PUNTO a) E' POCO CHIARO
- SUL PUNTO b) NON SONO D'ACCORDO PERCHE', NEL CASO PREVISTO, I TERZI INTERVENGONO COME RESPONSABILI DEL TRATTAMENTO O COME INCARICATI/AUTORIZZATI.
- SULL'ULTIMO CAPOVERSO NON SONO D'ACCORDO SUL FATTO CHE NON SERVA IL CONSENSO PER COMUNICARE I DATI AL MEDICO DI MEDICINA GENERALE. SU QUESTO PUNTO, RICORDO CHE IL PAZIENTE HA DIRITTO ALL'OSCURAMENTO DEI PROPRI DATI RIGUARDANTI LO STATO DI SALUTE NEI CONFRONTI DI QUALSIASI TERZO PROFESSIONISTA (MI RIFERISCO AL FSE/DOSSIER SANITARIO ELETTRONICO).
- NON VIENE FATTO ALCUN ACCENNO AL FSE/DOSSIER SANITARIO ELETTRONICO

Vitacca

- Può essere opportuno prevedere la possibilità di non acquisire il consenso in conformità a quanto previsto dall'art. 130 comma 4) d. lgs. 196/03 modificato dal d. lgs. 101/18: non necessità del consenso (ma della sola informazione) in caso di utilizzo de dati di contatto raccolti in sede di accettazione, per comunicazione in merito ai servizi offerti dal titolare. Infatti il comma 4) prevede: "Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, puo' non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, e' informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

- In merito alla condivisione dei dati con strutture e professionisti non appartenenti all'organizzazione del titolare (rif. 5.2.1. b) è opportuno precisare se in tali strutture e professionisti si includono soggetti a cui il titolare attribuisca incarico di Responsabile del trattamento nell'ambito di processi esternalizzati (in toto o in parte) come ad esempio service di laboratorio. In tal caso si ritiene non si concorda nel chiedere il consenso in quanto già operanti le basi giuridiche di cui al punto 3.2.2.3

Orsini - Perciballi

Meglio parlare di utenti ed eliminare la parola pazienti che circoscrive l'ambito ad una sola fattispecie.

Commentato [FFM62]: riportato

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Vitacca

Richiedere il consenso in casi come quello citato (es, service di laboratorio) comporterebbe la necessità di articolare i processi di accettazione in modo differenziato per le prestazioni ambulatoriali / diagnostiche eseguite internamente e quelle che richiedono l'invio all'esterno dell'esecuzione delle attività analitiche per parte o per la totalità degli esami richiesti.

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

5.3 Diritto all'accesso alla portabilità dei dati

a. Completezza

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Falcini

Tempi lunghi per un sistema repository unico.

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

5.4 Diritto alla cancellazione

a. Completezza

Mazzeo

Farei un maggiore riferimento ai casi (par. 3) in cui il diritto alla cancellazione può essere negato

Orsini - Perciballi

Sarebbe opportuno fare un distinguo tra la gestione analogica e quella digitale e/o digitalizzata, tenendo conto che nella gestione digitale i dati sono inviati al sistema di conservazione a norma che è un sistema terzo, chiuso e non accessibile. Di conseguenza è possibile prevedere la cancellazione dei dati dai verticali che gestiscono il singolo trattamento dato che gli stessi sono già stati riversati sul sistema di conservazione.

b. Correttezza

Mazzeo

Non ritengo che in TUTTI i casi di richiesta di cancellazione, la stessa vada declinata solo come indisponibilità e non accessibilità del dato

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Sammartino

NON E' CHIARO IL PENULTIMO CAPOVERSO "*LA CANCELLAZIONE RICHIESTA DALL'INTERESSATO VIENE IMPLEMENTATA NELLA NON DISPONIBILITA' ..... DISTRUZIONE FISICA DEI DATI STESSI*"

Commentato [FMF63]: E' evidenziato che la struttura dei sistemi informativi rende difficile l'applicabilità in tempi brevi di questi diritti dell'interessato, esplicitamente prescritti dal Regolamento.
A fronte di questa difficoltà è previsto solo un impegno del titolare a tenere conto di questa esigenza nei nuovi sviluppi ed a formalizzare la strategia adottata in un apposito docuemnto.

Commentato [FFM64]: Fermi restando diversi obblighi di legge, in caso di cancellazione il titolare è responsabile della cancellazione di tutte le copie dei dati personali interessati in suo possesso, incluso quindi nel sistema di conservazione

Commentato [FMF65]: E' opportuno esplicitare i casi in cui questa regola non è applicabile

Commentato [FMF66]: E' stato riformulato in modo da renderlo più chiaro.

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

5.5 Diritto alla rettifica

a. Completezza

Orsini - Perciballi

Andrebbe meglio specificata la differenza tra dato di salute, dato personale e "valore" in quanto sembrano essere utilizzati in maniera indefinita. In particolare suggeriamo di consentire all'interessato di rettificare i dati personali relativi ad esempio alla residenza ai recapiti telefonici email e quant'altro; Mentre nel caso di segnali biometrici e/o di diagnosi ci sembrerebbe più opportuno parlare di integrazioni che non di vere e proprie rettifiche.
Suggeriamo altresì di specificare che cosa si intende con la parola "valore".

Commentato [FFM67]: Eliminato il termine "valore"

Commentato [FFM68]: Può trattarsi anche di rettifiche/variazioni di dati precedentemente trasmessi

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

5.6 Obbligo di notifica in caso di cancellazione o rettifica

a. Completezza

Iacono

Si fa riferimento al paragrafo 7.3 ma non mi sembra corretto (almeno non del presente documento)

Commentato [FMF69]: Corretto, il riferimento esatto è § 8.3

Orsini - Perciballi

La notifica di avvenuta modifica dei dati non deve avvenire in modo indiscriminato ma solo nel caso in cui la modifica stessa possa influenzare le decisioni cliniche/diagnostiche legate a successivi trattamenti e solo nel momento in cui sorga la necessità che questi trattamenti debbano essere messi in atto.

Commentato [FFM70]: Il Regolamento non prevede deroghe o limitazioni a questo obbligo di notifica. Inoltre il titolare non ha modo di sapere se/quando il dati rettificato sarà utilizzato da altri titolari a cui è strato trasmesso.

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Andrebbe specificata meglio l'applicabilità nei casi in cui il sistema informatico lo consenta

Cap. 6. Criteri per l'accesso ai dati

Iacono

Nel paragrafo 6.1.1.1 lettera a in fondo al secondo capoverso cambierei il verbo "viene" con "deve essere"

Commentato [FMF71]: aggiornato

Nel paragrafo 6.1.1.2 alle lettere a, b, d i riferimenti ai paragrafi 6.1.1.1 sono sbagliati (manca un 1)

Commentato [FMF72]: corretto

Nel paragrafo 6.1.1.3 lettera a cambierei "responsabilità paziente" con responsabilità del paziente"

Commentato [FMF73]: corretto

Nel paragrafo 6.1.2.1 dopo la parola l'accesso c'è una "a" da cancellare. Nell'ultimo capoverso la parola "pseudonimizzati" è sbagliata e il riferimento al paragrafo 7.5 è sbagliato.

Nel paragrafo 6.1.2.2 secondo capoverso il riferimento al paragrafo 7.5 è sbagliato

Nel paragrafo 6.1.4.1 alla lettera a secondo capoverso il riferimento al paragrafo 7.1.1 è sbagliato. Alla lettera b il riferimento al paragrafo 7.5 è sbagliato

Nel paragrafo 6.1.4.2 alla lettera a secondo capoverso il riferimento al paragrafo 7.1.2.2 è sbagliato. Alla lettera b terzo capoverso modificare "identificazione" con "l'identificazione". Sempre alla lettera b terzo capoverso c'è il riferimento al paragrafo 7.5 che non c'è.

Nel paragrafo 6.1.5.2 al primo capoverso si fa riferimento ai paragrafi 6.1.6.1a e 6.1.6.1b che non ci sono.

Commentato [FMF74]: coretto

Commentato [FMF75]: corretto (il riferimento è § 8.5)

Commentato [FMF76]: corretto

Commentato [FMF77]: corretto (i riferimenti sono ai § 8. ...)

Commentato [FMF78]: corretto, il riferimento è al § 6.1.5.1. ...

Vitacca

6.1.5 Trattamenti finalizzati alla gestione della infrastruttura tecnologica: 6.1.5.1 Tipologie di dati necessari: opportuno prevedere un punto c) nei casi di accesso ai dati è opportuno prevedere il caso di sviluppo dei sistemi ICT e integrazione con nuove tecnologie, prodotti, applicazioni di volta in volta acquisiti e implementati

Commentato [FMF79]: aggiunto

Perciballi - Orsini

Paragrafo 6.1.1.1 lettera a la frase "personale medico ed assistenziale" andrebbe sostituita con "personale sanitario". Questo da ripetere ogni qualvolta compaia detta espressione.

Commentato [FFM80]: E' presente una distinzione fra il personale medico ed assistenziale, responsabile di valutare lo stato di salute del paziente e definire/attuare gli atti sanitari necessari (che ha bisogno di accedere a tutti i dati disponibili) ed altro personale sanitario coinvolto nella sola esecuzione di una attività, che ha bisogno di vedere solo i dati personali rilevanti per l'attività stessa.

Nell'ultimo capoverso lettera a) si evidenzia che non sempre è obbligatorio comunicare gli stati di salute e situazioni che possono determinare rischi per la salute degli operatori infatti per legge gli operatori stessi dovrebbero sempre mettere in atto tutti gli accorgimenti di protezione individuale che evitino eventuali contagi e/o contatti con materiale biologico del paziente.

Commentato [FFM81]: Alcune informazioni non possono essere comunicate, per precisa disposizione di legge

Nella lettera e) il contenuto appare troppo generico.

Commentato [FFM82]: In questa sede è solo evidenziata la necessità di accedere a dati personali in questa tipologia di trattamenti, ulteriore dettaglio potrà essere specificato nella definizione delle singole procedure

Paragrafo 6.1.1.3 Sostituire "personale medico" con personale sanitario o personale preposto.

Alla lettera b) da rivedere in chiave di responsabilità della Direzione Sanitaria di presidio che è l'organo deputato, per legge, a valutare le richieste di esibizione e fornire copia conforme delle stesse.

Commentato [FFM83]: Cfr § 6.1.1.1

Commentato [FFM84]: E' stata aggiunta la eventuale necessità di autorizzazioni

6.2 Regole di protezione predefinita

a. Completezza

Baratto

Da approfondire….ho dubbi sui criteri di accesso ai dati , sia in rapporto con FSE e DSE sia perché non vengono tutelati adeguatamente i dati super sensibili/giudiziari. Cosa identifica la "Necessità" e/o l'opportunità..?

Caputo

Le situazioni di rischio degli operatori non possono portare a evidenziazioni se protette da normativa specifica (es HIV) e se relative a dati ultrasensibili/giudiziari

Vitacca

E' opportuno prevedere/precisare la possibilità di utilizzare tecniche di anonimizzazione dei dati semplificate rispetto a quanto previsto dal "Parere 05/2014 sulle tecniche di anonimizzazione" del 10/4/2014, redatto dal WP29.
Il parere indicato prevede complesse tecniche di anonimizzazione dei dati (randomizzazione e generalizzazione) giustificabili nella misura in cui si prevede il riutilizzo dei dati per finalità diverse da quelle esplicitate nel momento di prima raccolta, operando, in particolare, operazioni di interconnessione con altre fonti di dati che aumentano il rischio di individuazione dell'interessato.
E' quindi opportuno verificare la possibilità di prevedere modalità di anonimizzazione semplificate (es. semplice cancellazione dei dati anagrafici e codici univoci identificativi) che, pur non eliminando completamente il rischio residuo di identificazione del dato, possano comunque essere considerato accettabili dal Garante fintantoché il trattamento rientri tra quelli dichiarati dal codice di condotta.

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Vitacca

L'eventuale necessità di applicare tecniche complesse di anonimizzazione dei dati, soprattutto se necessarie per i trattamenti finalizzati ad analisi a supporto del titolare (rif. 6.1.3,1 a), rischia di essere inapplicabile in realtà organizzative non complesse o di esporle a possibili contestazioni in caso di utilizzo di modalità semplificate non opportunamente formalizzate dal codice di condotta.

Commentato [FMF85]: La "necessità" nelle varie tipologie di trattamento è definita al § 6.1. Eventuali situazioni particolari dovrebbero essere evidenziate in quel capitolo.

Commentato [FMF86]: aggiunto al § 6.1.1.1 : "compatibilmente con le disposizioni di legge applicabili"

Commentato [FMF87]: aggiunto il § 8.6 che prevede la documentazione da parte del titolare dei meccanismi di anonimizzazione e mascheramento adottati nei vari trattamenti con una valutazione del rischio circa la possibilità di individuazione indiretta

Commentato [FMF88]: cfr punto precedente

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Andrebbe descritto meglio il caso di collaborazione territoriale

Commentato [FMF89]: Da approfondire e dettagliare già nella prima versione del documento

6.3.1 Abilitazione individuale all'accesso ai dati – regole generali

a. Completezza

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Iacono

Alla lettera b quarto capoverso c'è la parola "totale" al posto di "titolare"

Commentato [FMF90]: corretto

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Andrebbe descritto meglio il caso dei sistemi legacy

Commentato [FMF91]: Si può dettagliare come allegato informativo nei casi di best-practices

6.3.2 Abilitazione individuale all'accesso ai dati – situazioni particolari

a. Completezza

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Iacono

Alla lettera C dopo "a solo titolo di esempio: - per quanto riguarda (è scritto per quanti riguarda). Ritengo che non sia chiaro il riferimento "o da un sistema informatico"

Commentato [FMF92]: riformulato

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Andrebbe descritto meglio il caso dei documenti cartacei

Commentato [FMF93]: Da approfondire e dettagliare già nella prima versione del documento

6.3.3 Abilitazione individuale all'accesso ai dati – attività eseguite senza l'ausilio di sistemi informatizzati

a. Completezza

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

Forse occorrono rinvii più chiari alle norme precedenti

Ferrara

Andrebbero forniti dei termini di riferimento rispetto ai scenari e processi tipici

Ravaioli

Andrebbe esplicitata meglio la casistica poiché la documentazione cartacea è molto presente ancora nelle Aziende Sanitarie. Andrebbe specificata l'obbligatorietà di una sorta di raccolta di "impegno alla riservatezza" con firma da parte degli operatori (in particolare mi riferisco al personale amministrativo che accede moltissimo anche trasversalmente slle UU.OO. ai dati di tutti i pazienti su cartaceo come al momento del rilascio dei referti) al momento della assunzione ad esempio

Commentato [FMF94]: da dettagliare nella versione definitiva

Cap. 7. Registri

7.1 Obiettivi e contenuti

a. Completezza

Caputo

Utile inserire un modello di riferimento

Commentato [FMF95]: esistono già modelli di riferimento diversi, definiti da parte di diverse Regioni.

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Iacono

Manca il riferimento del paragrafo alla terza riga. Il riferimento del paragrafo 7.1 alla lettera c è sbagliato

Commentato [FMF96]: corretto

c2. Applicabilità nel contesto dell'organizzazione

Falcini

Riferimenti regionali diversi

Ravaioli

Andrebbe a mio parere definito un modello nazionale di registro dei trattamenti ma ogni regione si è mossa autonomamente al momento

Commentato [FMF97]: negli allegati informativi potrà essere fatto il tentativo di omogeneizzare quanto già definito dalle diverse regioni

Vitacca

Si ritiene opportuno non aumentare ulteriormente la complessità e la numerosità delle informazioni da riportare nel registro dei trattamenti rispetto a quanto già previsto dall'art. 30 del Regolamento. L'aumento della complessità del registro comporterebbe sicuramente notevole complicazione nell'elaborazione/ricerca di programmi software (che mettano in relazione i trattamenti, tempi di conservazione, finalità e basi giuridiche, categorie di dati, destinazione dei dati, misure di sicurezza ecc.) da sviluppare internamente o da acquisire nel mercato.

Commentato [FMF98]: si tratta di informazioni già analizzate e gestite nell'ambito delle varie regole del codice. L'unificazione di queste informazioni nei Registri tende a semplificare il lavoro, evitando il proliferare dei documenti ed fornendo un punto di riferimento complessivo.

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Sarebbero opportuni dei template

7.2 Valutazione della liceità del trattamento

a. Completezza

Caputo

Mantengo sempre la necessità di affidare un ruolo più significativo al DPO

Commentato [FMF99]: Cfr commento generale circa un capitolo -in fase di elaborazione da un apposito gruppo- circa il ruolo del DPO

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Sarebbero utili dei riferimenti a scenari e situazioni specifiche

7.3 Modalità di tenuta

a. Completezza

Ravaioli

Andrebbe forse specificato che il registro va protocollato da parte del titolare del trattamento (Direttore Generale) nella versione più aggiornata ed integrato periodicamente (revisione ogni 6 mesi?). La periodicità della revisione formale del registro sarebbe utile se indicata poiché attualmente non c'è chiarezza sul tema

Commentato [FMF100]: Aggiunta la necessità di una procedura per l'aggiornamento del registro

Mazzeo

Inserirei un'indicazione circa il soggetto (Titolare, DPO ?) cui è affidata la tenuta del Registro

Commentato [FMF101]: E' previsto che il titolare definisca una procedura per la tenuta del registro, che quindi dovrà esplicitare il responsabile della tenuta del registro stesso.
La direzione deve approvare la procedura (§ 4.1)

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

Vale la pena di fare un punto a parte ?

Cap. 8. Sicurezza

8.1 Tipologie di sistemi informatizzati e relative esigenze

a. Completezza

Mazzeo

Ritengo che le indicazioni sul trattamento in forma cartacea siano troppo sintetiche. In ambito sanitario, paradossalmente, i maggiori rischi di diffusione/utilizzo non corretto delle informazioni si verificano sui documenti cartacei (cartelle cliniche e ambulatoriali, referti e immagini diagnostiche). La sicurezza intesa come indicazioni organizzative, in questo campo, dovrebbe essere maggiormente valorizzata

Commentato [FMF102]: E' un aspetto che andrà approfondito e dettagliato già prima della finalizzazione della prima versione del codice

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli

Difficilmente applicabile per la gamma dei dispositivi medici

Commentato [FMF103]: Costituiscono una componente fondamentale del sistema ed uno dei principali elementi di rischio, come emerso anche dalle recenti indagini effettuate sull'argomento, nell'ambito dell'iniziativa.

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

Considerare insieme i dispositivi medici rende poco attuabile l'indicazione

Commentato [FMF104]: I dispositivi ormai fanno strettamente parte del sistema. Non considerarli lascerebbe il codice troppo incompleto.

Ferrara

Sarebbero opportuni riformamenti di esempio

8.2 Identificazione dell'utente

a. Completezza

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli

Attualmente non esiste un aggiornamento in tempo reale tra utenti abilitati ed ufficio personale per cui è difficoltosa la disabilitazione dei profili per cambio mansione o interruzione del rapporto di lavoro con l'Azienda

Commentato [FMF105]: L'esigenza va comunque prevista, anche secondo le citate normative dell'AgID

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Sarebbero utili esempi a scenari tipici con sistemi di vecchia generazione

8.3 Registrazione degli accessi e delle attività

a. Completezza

Sammartino

NON SI FA RIFERIMENTO ALL'OBBLIGO DI CONSERVARE IL FILE DI LOG PER UN DETERMINATO PERIODO (NELLE LINEE GUIDA PER IL DOSSIER SANITARIO ELETTRONICO) E' MENZIONATO L'OBBLIGO DI CONSERVARE IL FILE DI LOG PER ALMENO 24 MESI

Commentato [FMF106]: Specificato che va mantenuto per lo stesso periodo di conservazione dei dati

Mazzeo

Occorre specificare che in ambito sanitario, giusti provvedimenti del Garante, la tracciatura dei log è obbligatoria

Commentato [FMF107]: E' esplicitato l'impegno del titolare per quanto riguarda i sistemi di nuova realizzazione

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli

Il sistema informativo impiegherà tempo per adeguarsi

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

8.4 Sicurezza e ripristino dei dati

a. Completezza

Mazzeo

Manca un richiamo espresso (essenziale) all'obbligatoria effettuazione di prove periodiche di ripristino dei dati sottoposti a backup

Commentato [FMF108]: Descritto meglio il significato e le implicazioni della regola, indipendente dalle usuali procedure di backup-

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Sarebbero utili esempi a scenari tipici con sistemi di vecchia generazione

8.5 Pseudonomizzazione

a. Completezza

Caputo

Manca la sezione della ricerca, dove in alcuni casi la pseudonomizzazione è complessa (cfr immagini)

b. Correttezza

Baratto

Il criterio indicato per crittografare, riportato nel documento, "algoritmo basato su chiave asimmetrica di lunghezza minima di 2048 bit", risulta di difficile attuazione e comporta investimenti costosi (applicativi, tempo uomo etc.) ...valutare un altro criterio o lasciare al titolare la scelta della soluzione di crittografia più adeguata alle sue esigenze, tra quelle presenti sul mercato.

Manca un'apposita sezione dedicata alla ricerca dove la pseudonimizzazione è a volte complessa (ad es. immagini).

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Iacono

Al secondo capoverso quarta riga scrivere "presenza di dati" in vece di "presenza dati"

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara

Sarebbero utili esempi a scenari tipici con sistemi di vecchia generazione e gestione di dati multimediali

Commentato [FMF109]: La variabilità dei formati e delle tecnologie non rende possibile definire una unica regola. E' specificato che il titolare deve analizzare e documentare i meccanismi adottati nei singoli casi.

Commentato [FMF110]: E' un requisito minimo di sicurezza, implementabile con algoritmi e programmi disponibili open source, gratuitamente

Commentato [FMF111]: La variabilità dei formati e delle tecnologie non rende possibile definire una unica regola. E' specificato che il titolare deve analizzare e documentare i meccanismi adottati nei singoli casi.

Commentato [FMF112]: corretto

8.6 Ambienti di sviluppo, test ed addestramento

a. Completezza

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

Iacono

Al secondo capoverso quarta riga scrivere "presenza di dati" in vece di "presenza dati"

Commentato [FMF113]: corretto

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

8.7 Gestione dell'infrastruttura tecnologica

a. Completezza

Mazzeo

A mio parere sarebbe utile un richiamo anche alle misure di cui all'abrogato allegato b al Codice privacy che, in ogni caso, rappresentano uno "standard" applicato da sempre in privacy e al di sotto del quale non è possibile scendere.

Commentato [FMF114]: Nella versione definitiva, prima del suo consolidamento, è prevista l'integrazione del testo con tutti i riferimenti normativi rilevanti.

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli
Il registro sui VPN è importante ma difficilmente applicabile se con valore retroattivo

Commentato [FMF115]: e' un richiamo ad una norma già esistente

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ferrara
Sarebbero utili esempi a scenari che prevedono il coinvolgimento di diversi fornitori

Ravaioli
La tempistica dei 12 mesi indicati per l'adeguamento sarebbe a partire da quando?

Commentato [FMF116]: specificato: dall'adozione del codice da parte dell'organizzazione

8.8 Sanificazione digitale

a. Completezza

Mazzeo
Specificherei qualche elemento (es. per l'informatica standard di riscritture raccomandate per una cancellazione sicura dei dati)

Commentato [FMF117]: Specificato il riferimento a standard e linee guida consolidate

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

Ravaioli
In caso di manutenzione probabilmente sarebbe difficile cancellare i dati contenuti (es. ecografi)

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

8.9 Comunicazioni / invio di documentazione

a. Completezza

Mazzeo

Come già detto trovo sottostimata la necessità di fornire indicazioni sul trattamento cartaceo dei dati

Commentato [FMF118]: Cfr commento precedente

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ravaioli

Farei i vari casi:

1) scambio di mail fra dipendenti contenenti dati sensibili: indicazione a mettere in sicurezza lo scambio di mail tra utenti con mail aziendali. Direi che in generale dovrebbe passare il concetto che il sistema di scambio mail (es Zimbra) dovrebbe prevedere dei meccanismi di sicurezza insiti nella propria configurazione in modo che possano essere scambiati dati all'interno dell'azienda senza ulteriori passaggi (es criptazione file e invio pw), che risultano difficoltosi da mettere in atto per il personale (in Romagna questo sistema non viene accettato dai dipendenti
che lamentano di doversi scambiare continuamente dati sensibili via mail).
2) Invio di dati sensibili a mail esterna di un dipendente o di un utente : in questo caso sarà necessario criptare il file
3) Rimane aperta la questione delle modalità di utilizzo della PEC e del FAX per lo scambio di dati sia all'interno che all'esterno

Commentato [FMF119]: Sono aspetti che saranno approfonditi prima del consolidamento della prima versione del codice.

4) Fortemente richiesta dal personale è una indicazione a come scambiarsi le "consegne" nel reparto su supporto informatizzato (Cartelle condivise su server aziendale? Oppure ad es appositi spazi sulla cartella informatizzata?)

8.10 Gestione di documenti cartacei

a. Completezza

Mazzeo

Appare indispensabile fornire indicazioni almeno di massima sulla gestione della documentazione cartacea al di là del semplice richiamo alla necessità di stabilire delle regole. Occorre specificare, in particolare, come conservare i documenti, dove, come effettuare la movimentazione, in particolare, delle cartelle cliniche soprattutto in caso di trasferimento dei pazienti fra strutture diverse/reparti diversi.

Commentato [FMF120]: Sono aspetti che saranno approfonditi prima del consolidamento della prima versione del codice.

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

C'è già un riferimento analogo 6.3.3

Ferrara

Sarebbero utili esempi a scenari tipici

Cap. 9. Valutazione d'impatto sulla protezione dei dati

9.1 Ambiti di applicazione

a. Completezza

Baratto

Utile fornire, a titolo esemplificativo e non esaustivo, eventuali casistiche.

Caputo

Utili esemplificazioni e suggerire di identificare casistiche con il gruppo di lavoro

Ferrara

Sarebbe utile una maggiore descrizione del concetto ed il riferimento a linee guida e criteri esistenti (cfr sito garante)

Ferrari

A pag. 50 nel § 9.1 dopo il punto c) si suggerisce l'aggiunta di un punto:
"… d) che tenuto conto delle regole organizzative interne, e, delle modalità operative concrete, possano presentare comunque un livello di rischio medio-alto, implicando per il Titolare e/o i Responsabili un'attenta valutazione.

Mazzeo

Occorre un riferimento esplicito al provvedimento del Garante "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" dell'11 ottobre 2018

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

Commentato [FMF121]: Questo tema dovrà essere oggetto di approfondimento già prima del consolidamento della prima versione del codice

Commentato [FMF122]: aggiunto

Commentato [FMF123]: aggiunto

Da considerare nella valutazione dei rischi punti 4.5 ???

Ravioli
Sarebbe molto utile se le valutazioni di impatto venissero condivise a livello almeno regionale per facilitare la loro esecuzione e l'adozione di un modello comune di valutazione

9.2 Modalità di esecuzione

a. Completezza

Mazzeo
Suggerirei un riferimento all'utilizzo del software della CNIL

Commentato [FMF124]: aggiunto

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Ravioli
Ribadisco che sarebbe molto utile se le valutazioni di impatto venissero condivise a livello almeno regionale (es in un portale e al tavolo dei DPO) per facilitare la loro esecuzione e l'adozione di un modello comune di valutazione

9.3 Riesami periodici

a. Completezza

b. Correttezza

c. Valutazione e osservazioni in termini di usabilità

c1. Chiarezza dell'esposizione

c2. Applicabilità nel contesto dell'organizzazione

c3. Opportunità di specifica a maggiore livello di dettaglio attuativo

Falcini

La valutazione del rischio deve essere più organica all'audit e alla valutazione delle azioni

Ravaioli

Eventualmente nei casi più problematici dopo la DPIA indicare l'esecuzione di audit interni

Ulteriori considerazioni non legate a specifici punti del codice

Commentato [FMF125]: Questi contributi saranno oggetto di approfondimenti nel prossimo raffinamento

Andreoli

- nella pag. 16 sono citati gli artt. 75 – 93 che comprendono alcuni articoli abrogati dal D. Lgs. n. 101/2018;
- nella pag. 26 è citato il paragrafo 3.4 che non ha corrispondenza nei precedenti paragrafi;
- per quanto riguarda gli accessi del personale della struttura informatica o dei soggetti esterni che si avvale sarebbe stato opportuno citare gli Amministratori di Sistema, con obbligo del Titolare di definire l'ambito di operatività e/o di trattamento di ciascun Amministratore di Sistema,

facendo riferimento anche alle competenze delle professionalità ICT descritte dalle "Linee Guida per la qualità delle competenze digitali nelle professionalità ICT", adottate dall'Agenzia per l'Italia Digitale per l'anno 2017 (e/o alle successive stesure di tale documento); Magg. Inf. https://www.agid.gov.it/sites/default/files/repository.../linee_guida_-professioni-ict.pdf

- Infine, per quanto di riguarda gli accessi informatici ai dati sanitari da parte delle diversi professionisti e per le diverse finalità (sanitarie, amministrative) sarebbe stato opportuno citare, come avviene per il Dossier Sanitario, che "Devono essere, pertanto, preferite soluzioni che consentano un'organizzazione modulare dei dati, in modo tale da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al modulo di dati) indispensabili al raggiungimento dello scopo per il quale è stata consentita l'accessibilità".

Bruno

La enorme difficoltà di relazione con la maggior parte dei contraenti (esterni) che svolgono attività che comportano trattamenti di dati personali 'per conto' del Titolare, che quindi – loro malgrado – devono assumere un ruolo nella gestione privacy (generalmente Responsabile dei Trattamenti, con le modalità di cui all'art. 28).

Non è sempre scontata la competenza privacy presupposta dall'art. 28 per i soggetti a cui il Titolare deve ricorrere, ma, sia pure ammettendo il possesso di tale requisito, si tratta spesso di intervenire in corso d'opera in contratti abbondantemente decollati, e quindi non è facile trovare una soluzione abbastanza compliant col Regolamento.

Per queste ragioni ho proposto alla Direzione Generale l'istituzione di una misura organizzativa interna consistente nell'obbligo di validazione da parte del RPD di atti di gara o di qualsiasi provvedimento avente come finalità l'esecuzione di attività con rilevanza privacy da effettuare in partenariato con qualsiasi soggetto esterno: questo per garantirsi preventivamente l'esistenza della competenza privacy presupposta (così come avviene per i requisiti economici e tecnici) nonchè per preci

Caputo

Sezione 3.2 (trattamenti): nel caso di decesso, la separazione dei dati deve avvenire solo in caso di conoscenza del decesso da parte del titolare; non devono essere imposti obblighi di aggiornamento per soggetti che non hanno questo obbligo.

Accountability: Appare utile per tutti cercare strumenti e metodi comuni per garantire questo aspetto così rilevante.

Ferrara

a) definizione dei criteri di validità generale secondo cui individuare i ruoli di "responsabile del trattamento" e "titolare del trattamento", con riferimento alle strutture autonome che erogano indipendentemente servizi sanitari per conto di altre strutture (es. laboratori centralizzati a supporto di diversi centri)

b) descrivere il contesto di collaborazione territoriale dal punto di vista organizzativo e dei processi/ruoli dei vari attori nella cura del paziente.

Luciani

Si suggerisce di inserire allegati che consentano di focalizzare in maniera schematica un efficace **piano di *governace*** delle attivita' finalizzate all'adeguamento dell'organizzazione aziendale al regolamento europeo 2016/679 (GDPR) in materia di protezione dei dati personali.
Ad esempio:
 Modelli di checklist (data inventory) per:

- Ricognizione e registro dei sistemi che trattano dati sensibili all'interno delle organizzazioni (distinti per "centralizzati", "condivisi", "individuali") e comunque di tutti gli asset tecnologici
- Ricognizione e registro delle categorie di dati personali trattati ai fini della strutturazione del Registro delle attività di trattamento (del Titolare)
- Ricognizione e registro delle categorie dei trattamenti ai fini della strutturazione del Registro delle attività di trattamento (del Responsabile)

Ravaioli

Ritengo importante una più dettagliata analisi della sezione sulla Ricerca

Mazzeo

Suggerirei di implementare una sezione destinata alle best practices sanitarie a tutela della dignità dei pazienti con un richiamo (da valutare quanto espresso) alle indicazioni operative che hanno maggior impatto nell'organizzazione delle strutture sanitarie e che potrebbero partire da quanto riportato a suo tempo dal Garante nel ben noto vademecum "Dalla parte del paziente. Privacy: le domande più frequenti" https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1812194

Commentato [FMF126]: Introdotto, in premessa, questo come obiettivo di evoluzione del documento

Pinelli

Le considerazioni sono sia di carattere generale che indicative di mancanze o punti di forza.

1. Si ribadisce l'importanza di aver intrapreso questo percorso concreto di definizione del Codice di Condotta previsto dal GDPR e che tale definizione sia promossa da fonte autorevole e rappresentativa.
2. Le modalità di approccio di questo Codice di Condotta richiedono una adozione su larga scala (da molte/tutte le Aziende) per acquisire robustezza perché, rispetto ad un approccio piuttosto rigido verso il quale sembra puntare il GDPR, questo Codice è volto a garantire una situazione di maggior equilibrio tra possibilità (tempi e costi) e priorità di intervento. Per dar forza a questo approccio, (del tipo "io ti dico di fare 100, se tu titolare decidi di fare 50 perché ritieni adeguato 50 lo puoi fare ma se poi succede qualcosa sono tutti affari tuoi") occorrerebbe una sua applicazione su larga scala per aiutare tutte le Aziende. Informative, Procedure, Formazione e Documentazione sono la chiave per tutelarsi.
3. Questa versione di Codice è utile se viene fornita alle Aziende come "linea guida", in modo che ogni Azienda la possa personalizzare e calare nel proprio contesto/organizzazione
4. Modalità di acquisizione del consenso (pag. 25): nel punto **b)** sarebbe opportuno puntualizzare che "firmato con firma digitale" vale per differenti sistemi di firma (es. CNS, e firma grafometrica)
5. Pseudonomizzazione (pag. 43): in questo caso l'approccio non è in linea con l'approccio complessivo del documento = si può attenuare la linea?
6. Necessità e criteri per l'accesso e l'utilizzo dei dati (§ 6 da pag. 27 in avanti): tra le casistiche manca il trattamento per finalità di indagine condotta dall'Autorità Giudiziaria
7. Utile, strategica, la riconduzione alle misure minime di sicurezza ICT, livello standard
8. Il documento è carente rispetto al tema di come viene assicurato il principio di "privacy by default"
9. Il documento è carente rispetto al tema di come l'interessato possa esercitare i diritti garantiti dal GDPR
10. Il documento è carente rispetto al tema delle ditte/fornitori o soggetti terzi incaricati di trattamenti

Commentato [FMF127]: Il documento è stato costruito da tutti i partecipanti con questo scopo, non entrando in dettagli e/o soluzioni specifiche rispetto a contesti organizzativi e/o tecnologici. E' comunque esplicita raccomandazione dell'Autorità cercare di dettagliare il più possibile le indicazioni a livello operativo, anche per rendere meno interpretabili ed le attività di verifica all'interno delle singole aziende

Commentato [FMF128]: Specificato il riferimento a tutte le tecnologie certificate

Commentato [FMF129]: E' esplicita indicazione dell'Autorità cercare di dettagliare il più possibile le indicazioni a livello operativo, anche per rendere meno interpretabili ed le attività di verifica all'interno delle singole aziende

Commentato [FMF130]: Specificato al § 6.1.1.3.b)

Commentato [FMF131]: E' descritto, per le varie tipologie di trattamento nel § 6, che può essere ulteriormente dettagliato alla luce della evidenziazione di casi che dovessero essere stati non previsti

Commentato [FMF132]: Sono aspetti che saranno approfonditi nell'evoluzione, possibilmente già prima del consolidamento della prima versione

Commentato [FMF133]: Cfr commento precedente