Convegno Annuale AISIS

Privacy e Sicurezza
A supporto dell'innovazione digitale in Sanità

Come un piccolo intervento del Garante ha aumentato la sensibilità di un'intera Regione

cause, effetti, criticità e soluzioni praticabili

Graziano de' Petris

Azienda Sanitaria Universitaria Integrata di Trieste

Responsabile dell'Ufficio Privacy e dell'Unità di Ricerca in Telemedicina

Vicepresidente dell'Associazione Privacy Information Healthcare Manager in Sanità

graziano.depetris@asuits.sanita.fvg.it

Torino, 12 e 13 ottobre 2017
Hotel NH Torino Centro

Ispezione, sanzione, effetti

come un intervento centrale può rendere virtuosa una realtà periferica

Prescrizioni del Garante

- Visibilità del dossier mediata da consenso
  - eliminazione delle sintesi cliniche
- Analisi dell’esistenza di eventuali altre fattispecie di dossier
- Comunicazione FSE per condivisione dati tra aziende sanitarie

Scadenze prescrizioni del Garante

- A 3 mesi – Oscuramento ed oscuramento dell'oscuramento del singolo episodio
- A 6 mesi – Limitazione della visibilità

  - Soltanto su chi ha prestato il consenso
  - Soltanto al professionista sanitario che ha in cura il paziente
  - Soltanto per il periodo in cui ha in cura il paziente

- Conseguenza → *riscrittura dell'informativa*
- Conseguenza → *rifacimento del consenso*
- Conseguenza → *informatizzazione del consenso*

Oscuramento singolo episodio

- Prescrizione a 3 mesi: messa in atto delle modifiche sw necessarie per l'oscuramento e per l'oscuramento dell'oscuramento del singolo episodio.
- Al 24/04/13 la Regione ha scritto al Garante chiedendo 3 mesi di proroga per il collaudo
- Del nuovo sistema Gestore del Consenso

Cronologia dal 2012

- Provvedimento 27/01/2013
- Costituzione di un gruppo di lavoro e coordinamento regionale multidisciplinare
- Prescrizione a 3 mesi scadenza 27/04/2013 → richiesta proroga di 3 mesi → 27/07/2013
- Prescrizione a 6 mesi scadenza 27/07/2013 → messa in atto prima versione, richiesta proroga di 2 mesi per le ulteriori restrizioni

Adempimenti correlati

- Messa a norma dei bug privacy sui sistemi
- Gestione delle esenzioni sull'anagrafe unica regionale

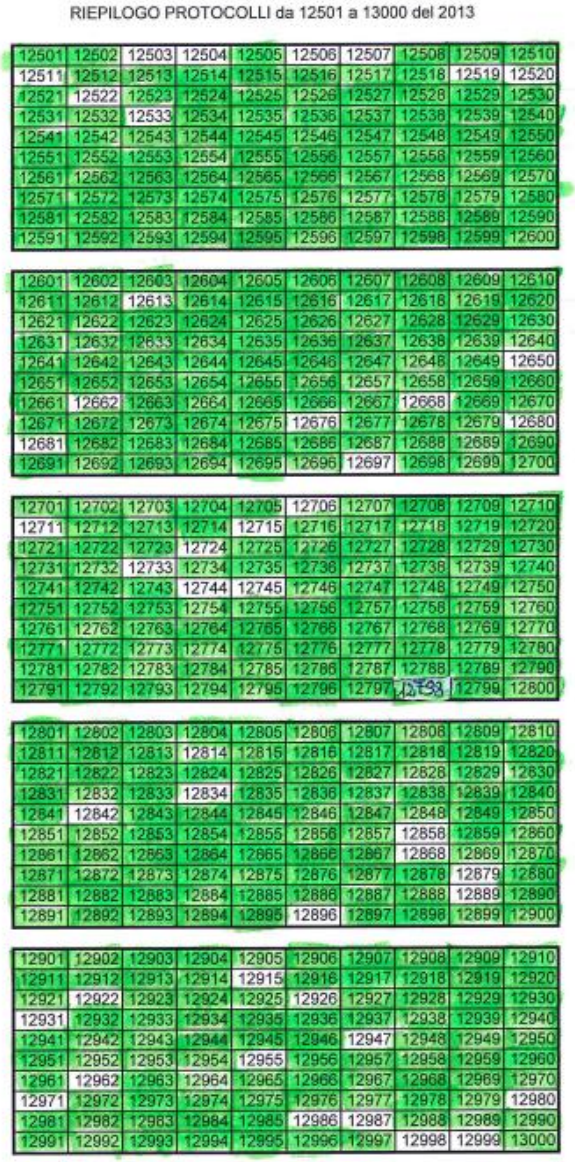
esempi

- Esenzioni sul sistema cup
- Accessi incrociati anatomie patologiche
- Visibilità multiazienda di alcune categorie di dati
- Verticali di servizi condivisi accessibili da più reparti (radiologia, laboratorio analisi…)

Dossier mediato da consenso

- Analisi dello stato della raccolta consensi
- Sopralluoghi nei reparti e formazione specifica on site
- Definizione di procedure e creazione di un ufficio di controllo dei consensi acquisiti
- procedura per la gestione dei casi di consenso errato
- procedura per l'archiviazione e la reperibilità dei consensi cartacei

Procedura consensi cartacei mancanti



RIEPILOGO PROTOCOLLI da 12501 a 13000 del 2013

12501	12502	12503	12504	12505	12506	12507	12508	12509	12510
12511	12512	12513	12514	12515	12516	12517	12518	12519	12520
12521	12522	12523	12524	12525	12526	12527	12528	12529	12530
12531	12532	12533	12534	12535	12536	12537	12538	12539	12540
12541	12542	12543	12544	12545	12546	12547	12548	12549	12550
12551	12552	12553	12554	12555	12556	12557	12558	12559	12560
12561	12562	12563	12564	12565	12566	12567	12568	12569	12570
12571	12572	12573	12574	12575	12576	12577	12578	12579	12580
12581	12582	12583	12584	12585	12586	12587	12588	12589	12590
12591	12592	12593	12594	12595	12596	12597	12598	12599	12600

12601	12602	12603	12604	12605	12606	12607	12608	12609	12610
12611	12612	12613	12614	12615	12616	12617	12618	12619	12620
12621	12622	12623	12624	12625	12626	12627	12628	12629	12630
12631	12632	12633	12634	12635	12636	12637	12638	12639	12640
12641	12642	12643	12644	12645	12646	12647	12648	12649	12650
12651	12652	12653	12654	12655	12656	12657	12658	12659	12660
12661	12662	12663	12664	12665	12666	12667	12668	12669	12670
12671	12672	12673	12674	12675	12676	12677	12678	12679	12680
12681	12682	12683	12684	12685	12686	12687	12688	12689	12690
12691	12692	12693	12694	12695	12696	12697	12698	12699	12700

12701	12702	12703	12704	12705	12706	12707	12708	12709	12710
12711	12712	12713	12714	12715	12716	12717	12718	12719	12720
12721	12722	12723	12724	12725	12726	12727	12728	12729	12730
12731	12732	12733	12734	12735	12736	12737	12738	12739	12740
12741	12742	12743	12744	12745	12746	12747	12748	12749	12750
12751	12752	12753	12754	12755	12756	12757	12758	12759	12760
12761	12762	12763	12764	12765	12766	12767	12768	12769	12770
12771	12772	12773	12774	12775	12776	12777	12778	12779	12780
12781	12782	12783	12784	12785	12786	12787	12788	12789	12790
12791	12792	12793	12794	12795	12796	12797	12798	12799	12800

12801	12802	12803	12804	12805	12806	12807	12808	12809	12810
12811	12812	12813	12814	12815	12816	12817	12818	12819	12820
12821	12822	12823	12824	12825	12826	12827	12828	12829	12830
12831	12832	12833	12834	12835	12836	12837	12838	12839	12840
12841	12842	12843	12844	12845	12846	12847	12848	12849	12850
12851	12852	12853	12854	12855	12856	12857	12858	12859	12860
12861	12862	12863	12864	12865	12866	12867	12868	12869	12870
12871	12872	12873	12874	12875	12876	12877	12878	12879	12880
12881	12882	12883	12884	12885	12886	12887	12888	12889	12890
12891	12892	12893	12894	12895	12896	12897	12898	12899	12900

12901	12902	12903	12904	12905	12906	12907	12908	12909	12910
12911	12912	12913	12914	12915	12916	12917	12918	12919	12920
12921	12922	12923	12924	12925	12926	12927	12928	12929	12930
12931	12932	12933	12934	12935	12936	12937	12938	12939	12940
12941	12942	12943	12944	12945	12946	12947	12948	12949	12950
12951	12952	12953	12954	12955	12956	12957	12958	12959	12960
12961	12962	12963	12964	12965	12966	12967	12968	12969	12970
12971	12972	12973	12974	12975	12976	12977	12978	12979	12980
12981	12982	12983	12984	12985	12986	12987	12988	12989	12990
12991	12992	12993	12994	12995	12996	12997	12998	12999	13000

Cosa fare nei casi in cui c'è un consenso inserito in Ge.Co. ma manca il riferimento cartaceo?

Procedura nel caso di registrazione in Ge.Co. su paziente sbagliato

- Caso 1: consenso registrato erroneamente su un paziente per il quale non era già stato registrato alcun consenso
- Caso 2: consenso registrato erroneamente su un paziente per il quale era già stato registrato un consenso standard
- Caso 3: consenso registrato erroneamente su un paziente per il quale era già stato registrato un consenso in emergenza e questo sia ancora attivo
- Caso 4: consenso registrato erroneamente su un paziente per il quale era già stato registrato un consenso in emergenza e questo non sia più attivo

Accesso al Dossier mediato da consenso

CONSEGUENZE negative su

- Attività routinarie su pazienti fisicamente non presenti e che non hanno ancora prestato il consenso
- Attività di consulenza ad professionisti esterni su pazienti fisicamente non presenti e che non hanno prestato il consenso
- Attività di critical review su pazienti deceduti
- Attività di critical review su gruppi di pazienti per patologia
- Attività di anatomia patologica su cadavere
- Attività di tesi/didattica/discussione su singoli casi o su patologie afferenti al singolo reparto
- Attività di direzione sanitaria
- …

Soluzione *parziale*

→maschera di autodichiarazione

A regime dal 27/07/2013

Criticità

NB: il caso di analisi di familiarità non è adeguatamente risolvibile

Esenzioni

- È stata tolta la visibilità

NB. Per la ricetta virtuale questo impedisce che l'esenzione possa essere compilata da chiunque non sia formalmente profilato "prescrittore"

Esenzioni CUP

- CUP
  - Tolta all'utente base la possibilità di modificare l'esenzione. Per modificarla l'utente deve avere un ruolo ad hoc
  - Visibilità della specifica dell'esenzione solo per gli abilitati del ruolo ad hoc

Oscuramento singolo episodio

- solo un ufficio ha il ruolo (la formazione e la responsabilità) per l'oscuramento
- solo la Direzione Sanitaria ha il ruolo di deoscuramento.
- organizzazione per la gestione dei moduli cartacei di richiesta di oscuramento e deoscuramento del singolo documento

Limitazione visibilità: solo chi ha in cura e solo per il tempo necessario

- Chiusura della visibilità sul dossier. non sono comunque visibili i dati anche dei pazienti che hanno espresso il consenso a meno che:
  - Il paziente non sia accettato in HIS
  - L'operatore non faccia autodichiarazione di necessità definendo le motivazioni e assumendosene la responsabilità

Attivazione Dossier

Chiamata Dossier

Verifica filtri: presenza paziente e struttura autorizzata (presa in carico)

NO

OK?

SI

Gestore Consensi per accesso dossier (esclusi eventi oscurati)

Percorsi di cura:

- Paziente ricoverato
- Paziente in PS
- Paziente esterno

Dossier

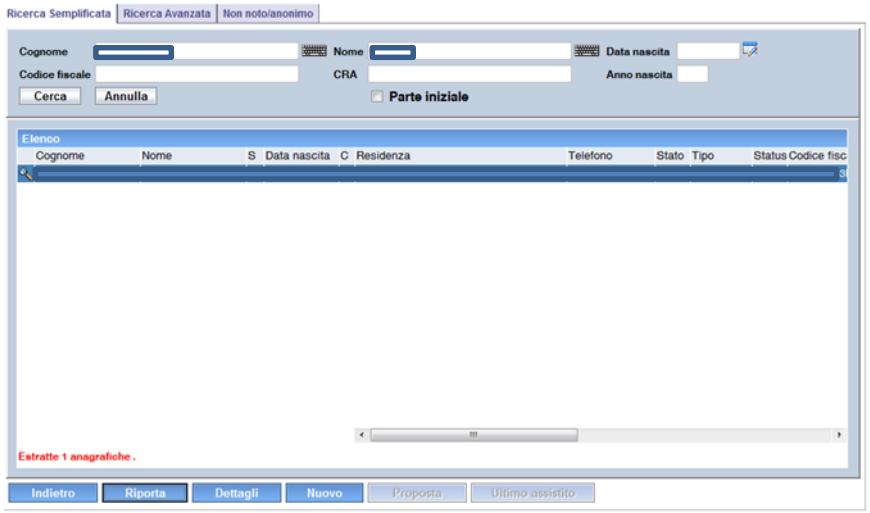
Limitazione visibilità: solo chi ha in cura e solo per il tempo necessario

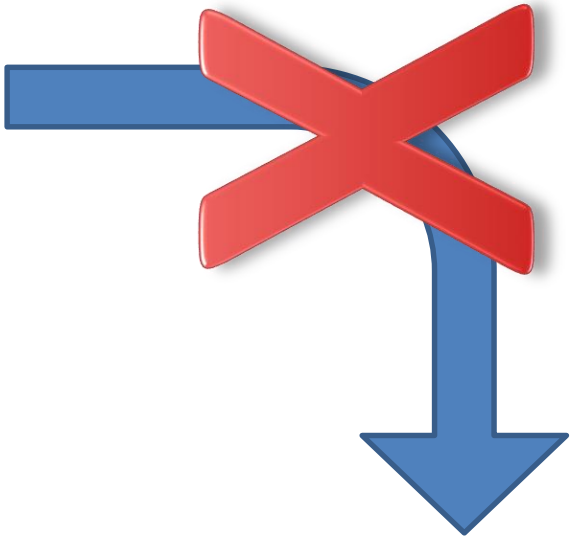
- Ricoverato: visibilità mediata da Ge.Co. + ADT
  - Chi: tutti
  - Quando: dal momento della accettazione del paziente come ricoverato in ADT al momento della dimissione da ADT

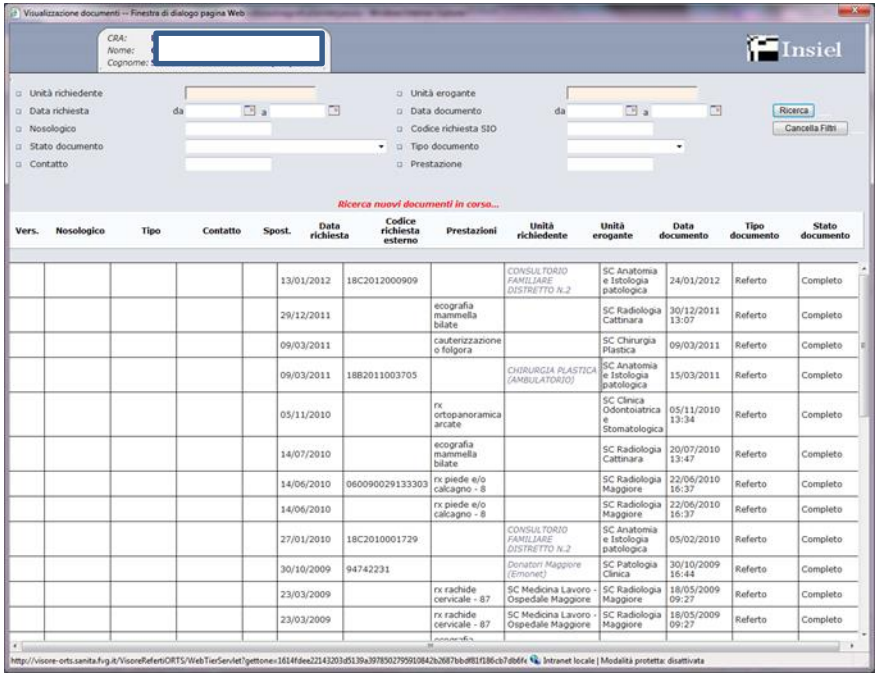
  - Percorsi di pre-ricovero in ADT per l'elezione
  - Il reparto può accettare in ADT se il paziente è in lista d'attesa (es. chirurgie)

Limitazione visibilità: solo chi ha in cura e solo per il tempo necessario

- In tutti gli altri casi → Autodichiarazione = Maschera tra l'identificazione del paziente e la presentazione della lista di documenti presenti, con cui chi è loggato si prende esplicitamente la responsabilità di accedere, per il tempo di sessione, motivando all'interno di una casistica predefinita, con in più la possibilità di mettere note


Ricerca Semplificata
Ricerca Avanzata
Non noto/anonimo
Cognome
Nome
Data nascita
Codice fiscale
CRA
Anno nascita
Cerca
Annulla
Parte iniziale
Elenco
Cognome
Nome
S
Data nascita
C
Residenza
Telefono
Stato
Tipo
Status
Codice fisc
Estratte 1 anagrafiche .
Indietro
Riporta
Dettagli
Nuovo
Proposta
Ultimo assistito




Visualizzazione documenti -- Finestra di dialogo pagina Web
Insiel
Unità richiedente
Data richiesta
Nosologico
Stato documento
Contatto
Unità erogante
Data documento
Codice richiesta SIO
Tipo documento
Prestazione
Ricerca
Cancella Filtri
Ricerca nuovi documenti in corso...
Vers.
Nosologico
Tipo
Contatto
Spost.
Data richiesta
Codice richiesta esterno
Prestazioni
Unità richiedente
Unità erogante
Data documento
Tipo documento
Stato documento
13/01/2012
18C2012000909
CONSULTORIO FAMILIARE DISTRETTO N.2
SC Anatomia e Istologia patologica
24/01/2012
Referto
Completo
29/12/2011
ecografia mammella bilate
SC Radiologia Cattinara
30/12/2011 13:07
Referto
Completo
09/03/2011
cauterizzazione o folgora
SC Chirurgia Plastica
09/03/2011
Referto
Completo
09/03/2011
18B2011003705
CHIRURGIA PLASTICA (AMBULATORIO)
SC Anatomia e Istologia patologica
15/03/2011
Referto
Completo
05/11/2010
rx ortopanoramica arcate
SC Clinica Odontoiatrica e Stomatologica
05/11/2010 13:34
Referto
Completo
14/07/2010
ecografia mammella bilate
SC Radiologia Cattinara
20/07/2010 13:47
Referto
Completo
14/06/2010
060090029133303
rx piede e/o calcagno - 8
SC Radiologia Maggiore
22/06/2010 16:37
Referto
Completo
14/06/2010
rx piede e/o calcagno - 8
SC Radiologia Maggiore
22/06/2010 16:37
Referto
Completo
27/01/2010
18C2010001729
CONSULTORIO FAMILIARE DISTRETTO N.2
SC Anatomia e Istologia patologica
05/02/2010
Referto
Completo
30/10/2009
94742231
Donatori Maggiore (Emonet)
SC Patologia Clinica
30/10/2009 16:44
Referto
Completo
23/03/2009
rx rachide cervicale - 87
SC Medicina Lavoro - Ospedale Maggiore
SC Radiologia Maggiore
18/05/2009 09:27
Referto
Completo
23/03/2009
rx rachide cervicale - 87
SC Medicina Lavoro - Ospedale Maggiore
SC Radiologia Maggiore
18/05/2009 09:27
Referto
Completo
Intranet locale | Modalità protetta: disattivata

Limitazione visibilità: solo chi ha in cura e solo per il tempo necessario

- NB: il Garante per questa maschera ha chiesto espressamente di associare un sistema di allarmi sui log (via mail/sms) affinché il Titolare possa monitorare l'andamento e presidiare il non abuso, sebbene non abbia definito gli indicatori (che restano quindi sotto la responsabilità dei Titolari).

Accesso per ricerca

- Per qualunque ricerca al di fuori di quelle per cui è previsto il passaggio attraverso il comitato etico è necessario che ci sia un documento di scopo firmato dal primario che indichi almeno il titolo della ricerca, lo scopo, le modalità, gli incaricati, la durata
- Gli incaricati devono essere incaricati per iscritto
- I dati devono essere anonimizzati prima possibile
- L'accesso ai dati ed il loro trattamento devono rispondere ai princìpi di ***pertinenza*** e ***non eccedenza***

Proposta ricerca

Risorse, Sensibilità, Investimenti

Sicurezza IT, Privacy e la fiaba di Cenerentola

Medical Device
Sicurezza IT e Privacy

perché sono inconciliabili e cosa possiamo fare

Un caso a caso
Primo atto

Procedura per l'acquisto RMN 3 Tesla

Allegato tecnico con prescrizioni puntuali: AgID, sicurezza IT, Privacy, regole interne, *tutto compliant*

Due possibilità :soluzioni 1 integrato in dominio e virtualizzato, soluzione 2 server e client fisici separati da vlan dedicata

Una ditta accetta la prima, questo gli permette di acquisire più punti e vince

Secondo Atto

In fase di installazione vogliono creare 4 utenti locali: 1 per accedere da fuori, 1 per accedere localmente, 1 per l'IT interna e 1 di scorta. Tutti con utente comune a tutte le installazioni. tutti i tecnici del mondo hanno un client sui portatili con lo stesso utente per tutti. Non si posssono installare le patch critiche di sicurezza, una volta l'anno lo farebbero loro da cd, selezionate da white list di casa madre.

L'Azienda sanitaria si irrigidisce e pretende il rispetto delle condizioni contrattuali

"*Nelle ultime 50 installazioni solo voi avete protestato*"

se il sw è sviluppato a norma e secondo le prescrizioni del produttore del SO, non ci sono mai problemi con le patch critiche, perché ci sono i controlli

Atto finale

dopo lunga discussione si contatta la casa madre che accetta senza problemi

CONSIDERAZIONI

- gli installatori locali seguono procedure standard, dalle quali non si discostano
- Le Aziende sanitarie non impongono le specifiche
- Il legislatore non ci aiuta
- Non si investe per formazione e aggiornamento dei tecnici IT delle aziende sanitarie

Telemedicina, Sperimentazioni, Ricerca

valore economico ed esistenziale del dato di salute

quali tutele?

Grazie dell'attenzione e buon lavoro

graziano.depetris@asuits.sanita.fvg.it