dott. Leonardo Sartori
Responsabile Servizio Sistemi Informativi

Trento, 22 ottobre 2015

L'organizzazione della privacy in APSS e il sistema dei controlli interni

leonardo.sartori@apss.tn.it

I sistemi informativi sanitari sono pervasivi, in Trentino oltre 70% dei cittadini ha almeno un contatto annuo nell'ambito dei percorsi assistenziali o sociosanitari con strutture o professionisti sanitari pubblici o accreditati

Il sistema informativo del Servizio Sanitario PAT è di notevole complessità organizzativa e tecnica

- l'ampiezza geografica – l'intera Provincia di Trento
- il gran numero di strutture fisiche e articolazioni organizzative APSS– 4 distretti, un dipartimento di prevenzione e un servizio ospedaliero provinciale con 7 presidi ospedalieri, dipartimenti ospedalieri e territoriali, circa 150 CdR, molti ambulatori territoriali, oltre 8300 dipendenti
- numerosi sistemi informativi, con applicazioni, basi dati e meccanismi di integrazione con sistemi provinciali e nazionali;
- 6.300 Pdl con oltre 9.500 incaricati di cui il 20% non dipendente APSS
- 190 applicazioni censite in esercizio di cui 16 critiche, 400 tra server fisici e virtuali
- infrastruttura di rete ampia e articolata (WAN, LAN, Wireless,) – 115 collegamenti interni e 200 esterni (RSA, MMG/PLS, farmacie territoriali, strutture accreditate ospedaliere e sociosanitarie, ecc.)

SISTEMA INFORMATIVO del Servizio Sanitario PAT

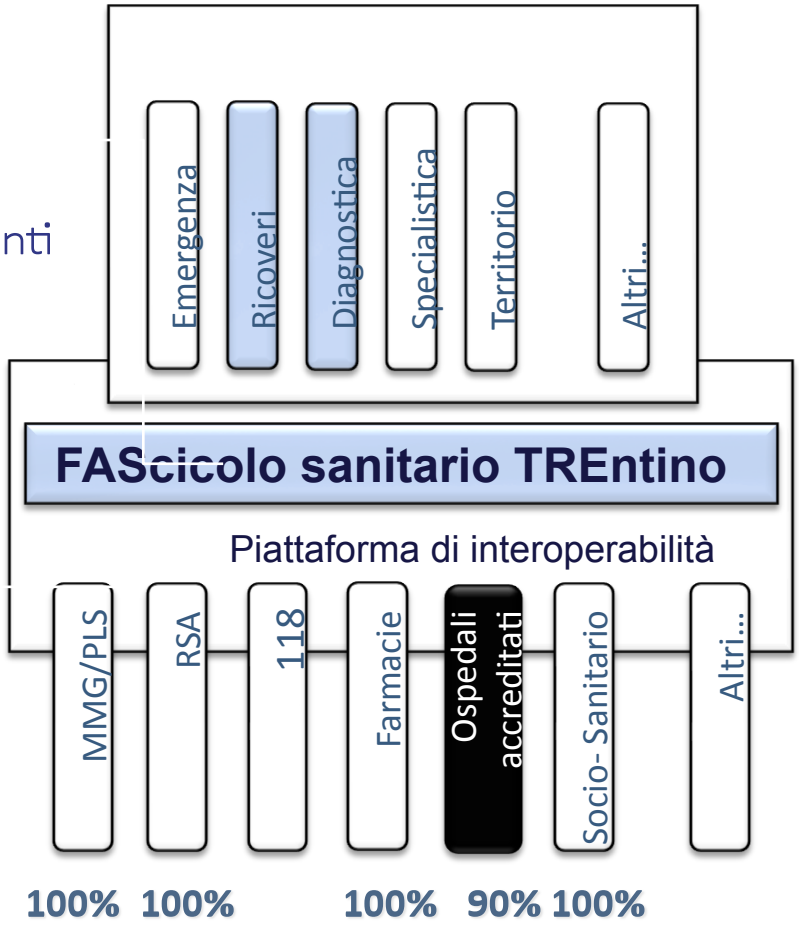
22.000.000 referti

59 milioni di documenti

2015

FSE

Ricetta specialistica dematerializzata
Patient summary



Integrazione 100% 100% 100% 90% 100%

4.689 utenti

Attività 2014:

- Ricoveri **1** **01.000**
- PS **2** **19.000**
- Referti ambulatoriali **6** **42.000**
- L. dimissione **94.000**
- Consulenze **194.000**
- ~~orde entry~~ **621.000**

SIO APSS e accreditate

FSE in Trentino

1 milione di msg di integrazione HL7/IHE al giorno

L'ecosistema di TreC

Servizio Sanitario Provinciale TrentinO

oggi gestiamo in Trentino almeno 6 tipologie di informativa e relativo consenso

generale *condivisione tra titolari del SSP (azienda sanitaria, MMG/PLS, strutture accreditate)*

di contatto *(ricovero, PS, ambulatoriale, etc.)*

FSE TreC *attivazione del FSE*

FASTTreC *accesso ai referti web online*

farmaceutica *accesso dei farmacisti alle ricette digitali non ancora erogate*

recupero referti *per passare i pregressi referti digitali in caso di cambio del MMG/PLS*

CONSENSO GENERALE

Il consenso di tipo generale - acquisito *una tantum,* nell'ambito della procedura di gestione integrata, avviata nel 2008, prevalentemente dal medico di fiducia dell'interessato oppure dagli uffici anagrafe dell'APSS all'atto della scelta o del cambio del MMG, ovvero espresso direttamente *on line* dall'interessato – soddisfa gli obblighi di legge per la maggior parte dei trattamenti effettuati per finalità di tutela della salute

la gestione integrata dell'informativa e consenso ad oggi ha raccolto 506.210 consensi (95% su 53.935 assistiti PAT)

- **46,1 % via Internet da MMG,**
- **37,6 % da cartella medico via messaggi Ampere,**
- **1,2 % via Internet da assistito,**
- **15,1 % da contatto**

CONSENSO DI CONTATTO

- Dal 2010 possibilità di esprimere il consenso generale anche in occasione di contatti con i servizi sanitari con modalità specifiche di negazione del consenso alla comunicazione verso il MMG/PLS di dati personali raccolti o esami effettuati o relativi esiti in occasione di **accesso al PS e/o di ricovero e/o di consulenza e/o di prestazioni ambulatoriali;**

- individuazione di casi comportanti il trattamento di dati sensibili che presentano rischi specifici e necessitano pertanto di un'informativa/ consenso ad hoc (nell'ambito di servizi quali SERT, Servizi psichiatrici, Consultori, Servizio di genetica ecc.);

- costruzione di un sistema di vigilanza e prevenzione attraverso registrazione, tracciatura (identificazione tramite *userid* dell'utente e chiave anagrafica del paziente) e conservazione dell'attività e degli accessi per i principali trattamenti sanitari aziendali.

Consensi generali e di contatto nei Sistemi Informativi Aziendali

590.029 contatti SIO - 2015 da 1 gennaio a 31 agosto

Ricoveri	***8.8 %***
PS	***21,5 %***
Ambulatori	***69,7 %***

Consensi di contatto

• ***consenso completo***	***583.434***	***98,88 %***
• ***solo struttura erogante***	***4.958***	***0,84 %***
• ***altro***	***1.637***	***0,28 %***

Oltre 75.000 aggiornamenti del consenso generale sono stati raccolti in contatti SIO, accettazione laboratorio o nei servizi di anagrafe sanitaria

REGOLE DI ACCESSO

- **L'accesso ai dati clinici è permesso solamente agli operatori incaricati e autorizzati dal Responsabile del Trattamento, per il solo espletamento delle operazioni di diagnosi e cura.**

- **L'accesso ai dati clinici è vincolato dalla presa in carico o dalla presenza di un contatto aperto o pregresso del paziente con la struttura sanitaria (per contatto si intende una qualsiasi richiesta di prestazione sanitaria: ricovero, accesso ps, esami laboratorio, visita specialistica, etc.)**

- **Se il contatto è antecedente di 180 gg. rispetto alla data di consultazione dei dati clinici, viene obbligatoriamente richiesta una motivazione per tale accesso.**

- **Se i dati clinici rientrano in una categoria di sensibilità particolare (IVG, HIV, …) viene obbligatoriamente richiesta una motivazione per accedervi.**

- **Se all'interno di un contatto vengono prodotti dei dati clinici con sensibilità particolare, tutti i dati relativi a quel contatto vengono classificati allo stesso livello.**

LIVELLO DI SENSIBILITA'

- **Per i trattamenti di valenza aziendale, come il Sistema Informativo Ospedaliero (SIO) nei casi indicati nell'elenco seguente viene attivato il livello di sensibilità, automaticamente o tramite intervento operatore; se all'interno di un contatto si verifica un evento che rientra nell'elenco, tutti i dati del contatto stesso acquisiscono tale livello di sensibilità.**
- **presenza di dati supersensibili riferiti ai seguenti casi:**
  - **Accesso per IVG**
  - **Accesso per HIV**
  - **Accesso per disturbi psichici**
  - **Accesso per gravidanza**
  - **Accesso per indagini genetiche**
  - **Accesso per malattie trasmissibili sessualmente**
  - **Accesso per tentato suicidio**
  - **Accesso per terapia metadonica**
  - **Accesso per TSO**
  - **Accesso di persone sotto copertura**
  - **Specifici esami di laboratorio**

MOTIVAZIONE ACCESSO

L'accesso ai dati clinici da parte degli utenti specificamente autorizzati può derogare dalla condizione "presenza di un contatto" in caso di rischio grave imminente ed irreparabile per la salute o l'incolumità fisica del paziente richiedendo in ogni caso una motivazione per tale attività secondo la sotto riportata tabella di alternative predefinite:

Motivazione Accesso dati clinici:

- Paziente in urgenza/emergenza
- Altra tipologia di urgenza (igienico sanitaria)
- Esigenze diagnostiche
- Riconciliazione anagrafiche pazienti
- Visita pre/post ricovero
- Richiesta da Autorità Giudiziaria/Polizia
- Verifica Controllo errori/anomalie
- Altra motivazione

Tutte le attività di consultazione dei dati clinici sono registrate su appositi archivi per la verifica di eventuali utilizzi impropri.

documentazione sanitaria digitale
Repository Referti

anno 2015 da 1 gennaio a 31 agosto : **oltre 30.000 accessi die da parte di 1.400 medici con 80% di accessi e altri 2.200 persone del ruolo sanitario**

5432 Registrazioni come dati supersensibili (0,85% dei casi)

565	***0,91%***	***Ricoveri***
34	***0,02%***	***PS***
4833	***1,14%***	***Ambulatoriale***

741.178 Consultazioni con motivazione (pari al 10%)

5519	**Paziente in urgenza/emergenza**
907	**Altra tipologia di urgenza (igienico sanitaria)**
567684	**Esigenze diagnostiche**
3565	**Riconciliazione anagrafiche pazienti**
22153	**Visita pre/post ricovero**
535	**Richiesta da Autorità Giudiziaria/Polizia**
2588	**Verifica Controllo errori/anomalie**
138227	**Altra motivazione**

SANITA' ELETTRONICA
nel Servizio Sanitario PAT

TreC Fascicolo Sanitario Elettronico ***https://trec.trentinosalute.net/***

Sono 51.737 i cittadini che hanno attivato il FSE attraverso la piattaforma TreC

FastTreC Referti Online ***https://trec.trentinosalute.net/***

Al 1 Ottobre 2015 85.186 cittadini hanno espresso uno specifico consenso per visualizzare online 213.017 referti di Laboratorio e Radiologia

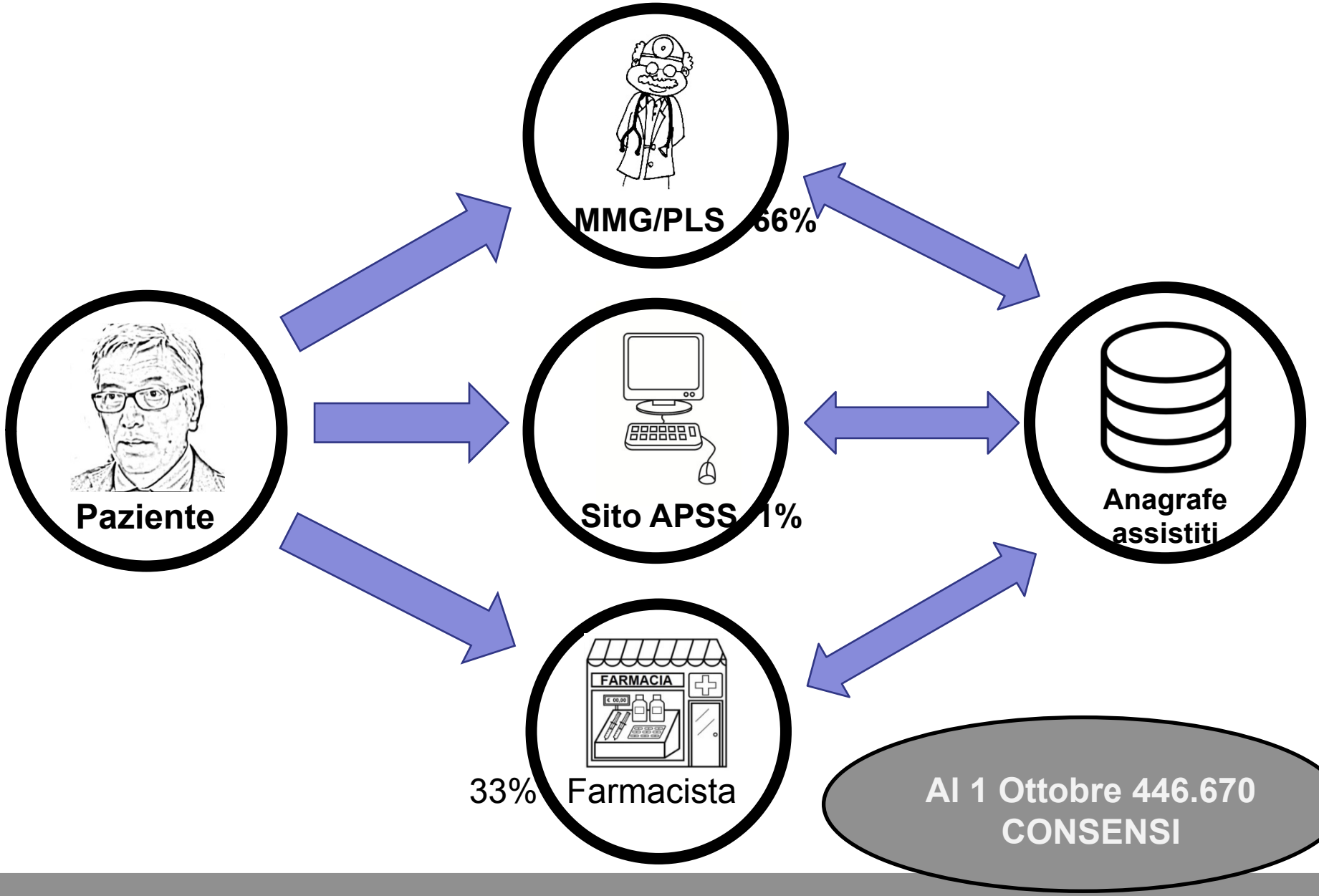
Ricette farmaceutiche

dal dicembre 2013 in PAT la ricetta farmaceutica è dematerializzata; per recarsi in farmacia senza ricetta cartacea gli assistiti esprimono un consenso preventivo per abilitare il farmacista all'accesso alle ricette farmaceutiche non ancora consumate; nei primi 8 mesi 2015 le ricette prodotte in Trentino sono state 3.124.383 di cui 88% digitali previa espressione di consenso da parte di 446.670 assistiti

recupero referti

Sono oltre 104.000 i consensi per trasferire i referti digitali in caso di cambio del MMG/PLS

CONSENSO RICETTA FARMACEUTICA DEMATERIALIZZATA



Gruppo per la Sicurezza Informatica e la Continuità Operativa SICO

- **Tra le iniziative adottate da SSI è la creazione di un apposito gruppo interdisciplinare denominato SICO (Sicurezza Informatica e Continuità Operativa) con compiti di analisi, consultazione e proposizione di azioni di prevenzione e miglioramento**
- **Il Gruppo è costituito da varie figure professionali informatiche come analisti, esperti di sistemi, reti, DBA, sicurezza, con i seguenti obiettivi:**
  - **proporre soluzioni e contromisure organizzative e tecniche volte a migliorare la sicurezza e la continuità in ambito ICT;**
  - **favorire l'introduzione in Azienda di metodi di analisi dei rischi, delle vulnerabilità, delle minacce per la valutazione del livello di sicurezza;**
  - **acquisire e strutturare informazioni aggiornate riguardo alle principali vulnerabilità e minacce; individuare e segnalare tempestivamente nuovi possibili rischi, minacce, vulnerabilità ICT (early warning);**
  - **relazionare circa lo stato della sicurezza e continuità ICT agli organi responsabili interni es. Gruppo Privacy, Responsabili di Trattamento;**
  - **fornire supporto a progetti e obiettivi specifici aziendali in ambito ICT;**
  - **avanzare proposte formative e di sensibilizzazione.**

Principali azioni ed interventi del SICO

- Piano di CO/DR
- Documentazione dei servizi critici
- Procedure di intervento - checklist
- Tecnologie e documentazione a supporto in caso di incidenti
- Formazione e aggiornamento continui del personale
- Test delle procedure di emergenza
- Audit continuo di sicurezza CASTORO
- Benchmark sulla disponibilità dei servizi ICT
- Indicatori di disponibilità dei servizi e di raggiungimento dei target
- Analisi delle vulnerabilità e proposta di contromisure
- Proposte organizzative per l'emergenza
- Certificazione interna CInQuE
- Revisione processo di IM secondo ITIL
- Survey sulla gestione degli incidenti ICT
- Revisione del processo di nomina dei RE di trattamento
- Piano e test di restore

Il piano di CO/DR

- **Il Documento Programmatico di Sicurezza DPS aziendale contiene il piano di sicurezza aziendale e indica le misure organizzative riguardanti la sicurezza e la privacy, i responsabili di trattamento, i trattamenti, la verifica delle abilitazioni, la nomina degli incaricati, l'osservanza delle misure di sicurezza. Il piano è aggiornato al 2012**
- **Il Piano di CO/DR redatto sulla base delle Linee guida per li Disaster Recovery nella PA ha fatto tesoro dei piani di continuità operativa e disaster recovery già redatti a partire dal 2005. Viene aggiornato annualmente**
- **I servizi ICT sono stati catalogati e valutati utilizzando lo strumento di autovalutazione di AgID**
- **Nel piano ricadono le attività di pianificazione organizzativa - quindi essenzialmente l'impiego delle risorse umane e delle conoscenze - da attivare e mobilitare in caso di emergenza e le procedure di intervento atte a garantire la continuità. Il piano contiene inoltre gli aspetti tecnici e tecnologici relativi al recupero e alla riattivazione di sistemi e delle infrastrutture**
- **Il piano è stato inviato ad AgID nel 2012 ed è stato approvato con alcune osservazioni; è stato aggiornato ed inviato nel 2013 e nel 2014**

Sistema di supporto e gestione degli incidenti CRASH

- **Il sistema CRASH (Continuity Reporter and Alerter for Security Helper) è il sistema di registrazione degli incidenti sviluppato all'interno di SSI e svolge le seguenti funzioni principali**
  - **Registrazione degli incidenti ed eventi rilevanti es. escalation**
  - **Procedura di triage dell'incidente**
  - **Procedure di intervento (checklist)**
  - **Segnalazione per via elettronica dell'accadimento (e-mail, sms, intranet)**
  - **Supporto all'attività del personale che gestisce l'incidente rubriche, documenti on-line, informazioni di supporto**
  - **Registrazione di attività rilevanti post incidente**
  - **Reporting delle informazioni raccolte**
  - **A breve, registrazione dei workaround e verifica del rispetto dei tempi nelle varie fasi della gestione incidente (SLA)**

CRASH: riepilogo incidenti registrati dal 10/9/2004 al 7/9/2015

Servizio	Moduli	Num. incid.	Durata tot	Durata media	% Indisp.	% Disp.	Target	Gap	OK NOK	Peso
Rete LAN / WAN principali	2	85	830:48:39	09:46:27	0,72	99,28	99,94	-0,66		0,33
Servizio di Backup / Restore	2	4	182:50:05	45:42:31	0,70	99,30	99,94	-0,64		0,75
Anatomia Patologica / Armonia	1	1	48:00:00	48:00:00	0,55	99,45	99,94	-0,49		0,00
PreleFarma	1	3	50:45:35	16:55:11	0,29	99,71	99,94	-0,23		0,67
Repository Referti	2	63	243:51:17	03:52:14	0,28	99,72	99,94	-0,22		0,83
Laboratory Information System	2	17	190:24:40	11:12:02	0,20	99,80	99,94	-0,14		0,88
Sistema Informativo Territoriale	9	17	51:58:05	03:03:25	0,15	99,85	99,94	-0,09		0,94
Casse, CUP, Accettazione LAB	1	12	64:15:00	05:21:15	0,10	99,90	99,94	-0,04		0,92
Radiology Information System	3	23	201:04:48	08:44:33	0,09	99,91	99,94	-0,03		0,65
Sistema Informativo Ospedaliero	2	45	164:16:30	03:39:02	0,08	99,92	99,94	-0,02		0,82
CUP	1	4	80:19:46	20:04:56	0,06	99,94	99,94	-0,00		1,00
Accettazione LAB	1	5	16:07:28	03:13:29	0,06	99,94	99,94	-0,00		0,80
Trasfusionale / Emonet	1	2	07:00:00	03:30:00	0,04	99,96	99,94	0,02		0,00
Documenti lavoro	1	2	47:29:00	23:44:30	0,04	99,96	99,94	0,02		1,00
Posta elettronica	2	12	66:40:31	05:33:22	0,04	99,96	99,94	0,02		0,92
Anagrafe Assistiti	2	16	43:52:12	02:44:30	0,02	99,98	99,94	0,04		0,88
Ser.T.	1	2	05:01:16	02:30:38	0,00	100,00	99,94	0,06		0,50
Rete Banda Larga	1	2	01:08:24	00:34:12	0,00	100,00	99,94	0,06		0,50
Halia - Catena esami di laboratorio	1	4	07:15:47	01:48:56	0,08	99,92	99,77	0,15		0,50
Atlante	1	1	01:40:15	01:40:15	0,02	99,98	99,77	0,21		1,00
Terapia intensiva e rianimazione	1	2	09:21:44	04:40:52	0,01	99,99	99,77	0,22		0,50
SIMFR Medicina fisica e riab.	1	1	00:37:39	00:37:39	0,01	99,99	99,77	0,22		1,00
Accesso Internet	1	2	04:13:42	02:06:51	0,00	100,00	99,77	0,23		1,00
Screening Mammografico	1	1	03:29:19	03:29:19	0,00	100,00	99,77	0,23		1,00
Sistema Archiviazione	1	1	01:02:59	01:02:59	0,00	100,00	99,77	0,23		1,00
EUSIS - Contabilità	1	1	00:32:37	00:32:37	0,00	100,00	99,77	0,23		1,00
SIGMA segreterie	1	1	00:47:00	00:47:00	0,00	100,00	99,54	0,46		1,00
		329	**2324:54:18**	**07:03:59**	**0,13**	**99,87**				

i registri informatici a supporto della gestione

- Nell'attività quotidiana e in caso di emergenza sono disponibili i seguenti "registri aziendali"
  - Tigre: elenco dei Trattamenti Informatizzati Gestiti (da SSI) e Regolarmente in Esercizio
  - Orsa: Organizzazione Registro Server Aziendali è l'archivio contenente le informazioni relative agli host; caratteristiche hardware, software, installazione e configurazione
  - Orca: Organizzazione Registro Collegamenti Aziendali in cui sono memorizzate le informazioni relative alla rete trasmissione dati per tipologia, area geografica, sede collegata, tecnologia, indirizzi sottoreti, stato attivazione
  - IPmanager: il registro che contiene gli indirizzi TCP/IP degli host aziendali; contiene anche informazioni sulle sottoreti e la loro distribuzione presso le sedi aziendali
  - GRU: Gestione Richieste Utente è l'applicazione che gestisce l'intero processo di raccolta, autorizzazione e soddisfacimento delle richieste utente; fornisce i report relativi alle abilitazioni e alla distribuzione delle PdL; **con più di 90.000 abilitazioni/disabilitazioni registrate e oltre 10.000 nel 2014 rappresenta il REGISTRO degli INCARICATI per ogni trattamento.**

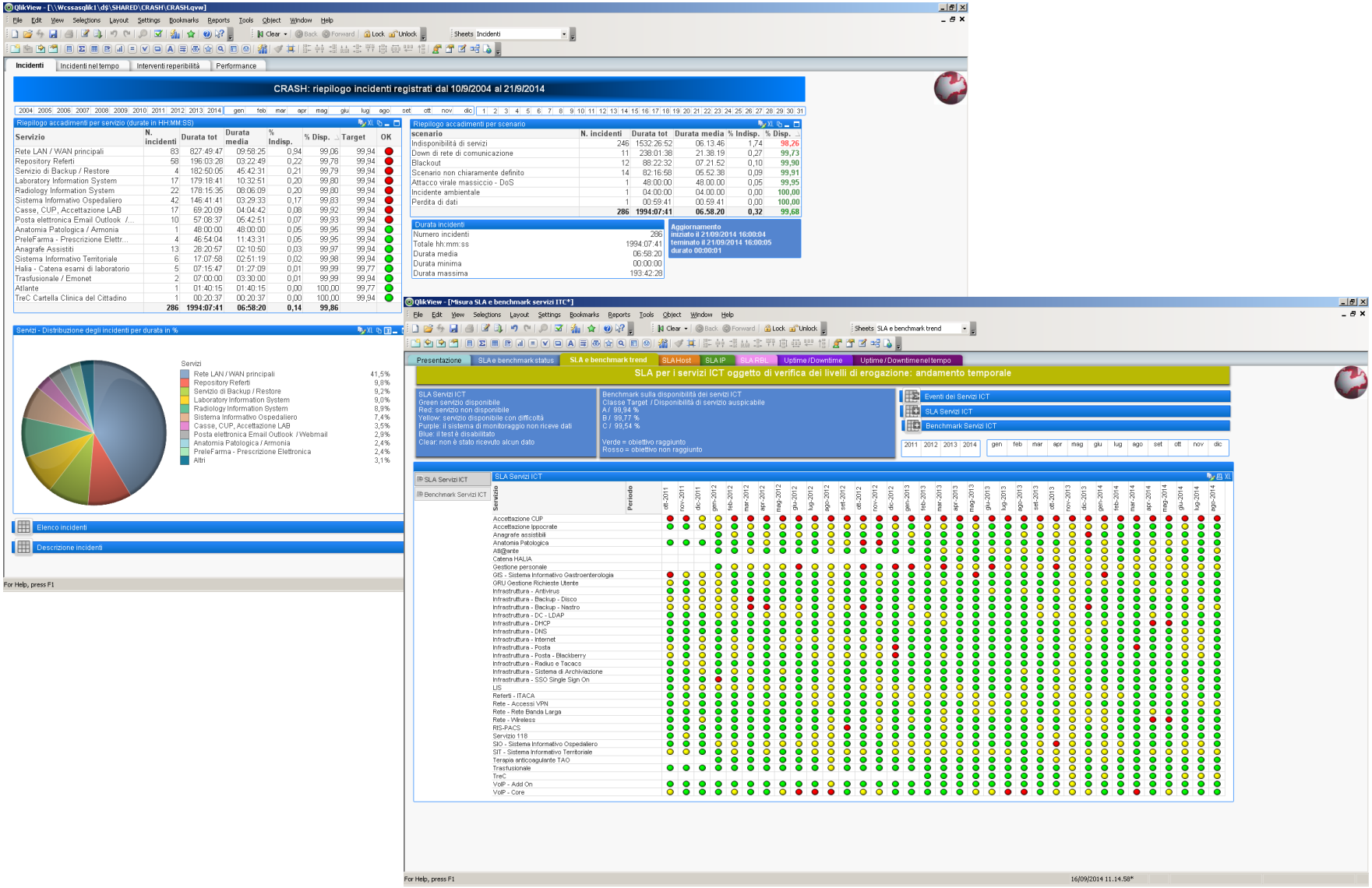
Formazione e aggiornamento continui del personale informatico

- Almeno due volte all'anno si tengono incontri di formazione e aggiornamento sui temi:
  - provvedimenti del Garante, decreti Ministeriali, Agid,.
  - Continuità operativa e disaster recovery
  - Documentazione dei servizi ICT
  - Organizzazione per la gestione degli incidenti e procedure di intervento
  - Utilizzo degli strumenti di monitoraggio e dei servizi di infrastruttura
  - Contributi dei referenti applicativi e degli AdS, novità intervenute di recente
  - Risultati dei test, degli audit, delle analisi delle vulnerabilità e delle contromisure

Audit continuo di sicurezza CASTORO

- CASTORO è l'acronimo di Cruscotto di Analisi della Sicurezza dei Trattamenti Operativi con Reportistica On-line

- E' un sistema che consente di registrare le informazioni relative allo stato di applicazioni delle misure minime ed idonee di sicurezza
- La compilazione di CASTORO è a carico degli AdS e dei Referenti applicativi di SSI; il sistema viene aggiornato almeno una volta all'anno
- Il sistema contiene un modulo di risk analysis che consente di registrare informazioni relative ai rischi, alla frequenza di accadimento di eventi negativi, all'impatto potenziale e di produrre dei report
- Le informazioni sono disponibili ai Responsabili di Trattamento
- Ha portato alla luce vulnerabilità relative a scarsa conoscenza delle politiche di sicurezza soprattutto da parte degli utenti finali (uso credenziali, screen saver, supporti rimuovibili)


QlikView - [\\Wcssasqlik1\dj$\SHARED\CRASH\CRASH.qvw]
CRASH: riepilogo incidenti registrati dal 10/9/2004 al 21/9/2014
Riepilogo accadimenti per servizio (durate in HH:MM:SS)
Riepilogo accadimenti per scenario
Durata incidenti
Servizi - Distribuzione degli incidenti per durata in %
Elenco incidenti
Descrizione incidenti
QlikView - [Misura SLA e benchmark servizi ITC*]
SLA per i servizi ICT oggetto di verifica dei livelli di erogazione: andamento temporale
SLA Servizi ICT
Benchmark sulla disponibilità dei servizi ICT
Eventi dei Servizi ICT
SLA Servizi ICT
Benchmark Servizi ICT

5 - Certificazione Interna di Qualità per la gestione delle Emergenze

- E' un sistema di certificazione interna volta a misurare:
  - la capacità di risposta, ovvero la propensione a farsi carico del problema e di offrire una soluzione;
  - la qualità della risposta, ovvero la capacità di offrire riscontri adeguati alla gravità ed estensione del problema;
  - la professionalità, in termini di rispetto degli standard procedurali e dell'assetto organizzativo aziendale;
  - il problem solving, ovvero la capacità di trovare e proporre nuove soluzioni, a fronte di criticità non previste o non conosciute;
  - il risultato, inteso come l'aver risolto o avviato la soluzione del problema e averne comunque ridotto al massimo l'impatto sull'utenza.

- Il certificato è personale, viene assegnato al personale che garantisce un adeguato livello comportamentale nell'arco di tre anni
- Il primo ciclo di certificazione si è concluso con un esame finale nel 2014

INCIDENTI INFORMATICI
SLA, tempi soglia e valori accettabili

Priorità	Servizi	SLA Presa in carico	SLA Tempo soluzione	SLA Tempo escalation	Casi
Major incident	Servizi critici	<15 min	<8 h	>30 min < 1h	90%
	Servizi vitali	<30 min	<8 h	>1 h < 1:30 h	90%
	Servizi delicati	<60 min	<8 h	>1 h < 1:30 h	90%
	Servizi non critici	<60 min	<8 h	>1 h < 1:30 h	90%
Minor incident	Servizi critici	<15 min	<12 h	>1 h < 1:30 h	80%
	Servizi vitali	<30 min	<12 h	>1 h < 1:30 h	80%
	Servizi delicati	<60 min	<16 h	>1 h < 1:30 h	80%
	Servizi non critici	<60 min	<16 h	>1 h < 1:30 h	80%

Questionario su incidenti ICT

- A luglio 2015 si è deciso di svolgere un sondaggio online presso i Responsabili di Servizi e UU.OO. per valutare il peso degli incidenti ICT sull'operatività e per verificare anche la presenza di procedure in grado di sostituire le procedure informatiche in caso di necessità
- Si è chiesto quali procedure in particolare vengono utilizzate dalle articolazioni organizzative, per quanto tempo il Servizio può operare in caso di incidente senza eccessivo degrado, come ci si è comportati nell'ultimo incidente e per quanto tempo si è riusciti a sopperire alla mancanza dell'ICT, se in caso di incidente e di perdita di dati sia necessario recuperarli e per quale intervallo di tempo sia possibile farlo, se si è mai verificata una perdita di dati
- Veniva inoltre chiesto se si riteneva il questionario utile e rispetto all'obiettivo di migliorare la gestione degli incidenti ed eventuali osservazioni di merito

Survey sulla gestione degli incidenti ICT

- Il survey si è concluso; i rispondenti che comprendono quasi tutti i responsabili di trattamento sono stati finora circa il 20% dei circa 150 soggetti coinvolti
- In generale l'accoglienza è stata buona e il questionario ritenuto utile anche se a volte complesso
- **Nelle risposte i tempi ritenuti necessari per la riattivazione dei servizi ICT è molto basso e prossimo a 0; alcuni servizi sono quindi ritenuti da tutti i rispondenti indispensabili e insostituibili es. RIS, SIO, LIS, anagrafe, PE, Internet**
- I prossimi passi saranno:
  - Verificare come effettivamente vengono utilizzati gli applicativi e convalidare i valori effettivi di RTO/RPO proposti dai rispondenti rispetto agli attuali
  - Individuare nuove soluzioni in grado di garantire i livelli di servizio necessari
  - Aggiornare in modalità condivisa le procedure alternative tecniche ed organizzative in caso di incidente
  - Comunicare un report che riepiloghi i risultati e gli interventi migliorativi

Revisione del processo di nomina Responsabili Esterni di Trattamento

- Nasce da un audit svolto presso i principali fornitori esterni che ha evidenziato lacune nel processo di nomina e aggiornamento:
  - le lettere di nomina erano vecchie e mai aggiornate
  - il disciplinare allegato era a sua volta obsoleto
  - i fornitori sembravano a volte non conoscere le norme e gli obblighi conseguenti
- E' stata svolta un'analisi, sulla base della quale è stato sviluppato un programma in fase di rilascio che compre tutte le fasi di nomina e rinnovo, di aggiornamento del disciplinare, di verifica di applicazione delle misure di sicurezza, di audit, di procedure di riconsegna e distruzione degli archivi a fine servizio
- A regime sarà utilizzato per gestire il rapporto con i fornitori di sistemi e soluzioni informatiche

Altre iniziative in corso

- Revisione del processo di creazione e revisione delle policy di sicurezza secondo ITIL
- Policies e procedure per l'utilizzo di device mobili aziendali e personali (servizio BYOD), Penetration test, gap analysis, piano di rientro
- Sistema di catalogazione degli incidenti ICT e Problem Management
- Nuovo audit presso i principali fornitori di servizi ICT, in particolare circa l'applicazione delle misure di sicurezza e l'esistenza di piani di continuità e DR

Prossimi passi

- *Standardizzare informative e consensi, perfezionamento della gestione del consenso per attuazione decreti "dossier e FSE"*
- *Estensione dei meccanismi di log e di tracciatura delle operazioni più significative per tutti i trattamenti critici*
- *Notifica via mail o SMS della disponibilità della ricetta digitale e del nuovo referto/documento sanitario dematerializzato*
- *comunicazione degli incidenti al livello nazionale*

- ***visibilità della tracciatura degli accessi e delle operazioni anche all'assistito via FSE TreC anche con alert***
- *Big data già oggi almeno 200 transazioni anno per cittadino via FSE , contemperare esercizio dei diritti e aspetti gestionali del contenzioso da tracciatura sui trattamenti .*

crescente complessità tecnologica e organizzativa

- *informare costantemente i cittadini via media e FSE e formare i professionisti (FAD, regole condivise,)*
- *adeguare e uniformare i sistemi informativi sanitari e sociosanitari attivando degli standard gestionali degli aspetti privacy, garantendo dei sistemi minimali di identificazione anagrafica degli assistiti e di definizione dei vari ruoli professionali.*
- *perfezionare l'interoperabilità dei livelli di ASL, regione e nazione, condividendo regole, ruoli e indicatori, garantendo dei sistemi minimali di identificazione anagrafica degli assistiti, di definizione dei vari ruoli professionali.*
- *adeguare i meccanismi di sicurezza per migliorare, in caso di usi non pertinenti, la gestione del contenzioso con assistiti e professionisti*

CONCLUSIONI

La gestione degli aspetti privacy è e sarà costosa e deve essere sostenibile per il SSN. Alla luce anche dei recentissimi decreti (FSE, dossier, 730 etc.), è opportuno un approccio organico e una standardizzazione delle modalità operative di gestione delle informative e di espressione del consenso a livello di singolo trattamento, di organizzazione sanitaria, regionale e nazionale.

Il cittadino deve poter essere attore protagonista della gestione dei propri dati sanitari digitali via FSE sia attraverso la gestione del consenso e l'oscuramento sia col controllo sulla tracciatura degli accessi e sulle operazioni più significative dei trattamenti .