



| Responsabili del trattamento dati | |
|--|-------------------------------------|
| Dipartimento Immagini | |
| S.C. Fisica Sanitaria Savona | Dr.Giovanni Ghiso |
| S.C. Medicina Nucleare Pietra Ligure | Dr.Luigi Bertolazzi |
| S.C. Neuroradiologia Diagnostica ed Interventistica P.L. | Dr. Riccardo Padolecchia |
| S.C. Radiologia Diagnostica Albenga | Dr.Riccardo Orlandi |
| S.C. Radiologia Diagnostica ed Interventistica P.L. | Dr.Giovanni Serafini |
| S.C. Radiologia Diagnostica ed Interventistica Savona- Cairo | Dr. ^{SSA} Angelina Cavallo |
| S.C. Radioterapia Savona | Dr.Corrado Marziano |
| S.S.D.Angiografia e Radiologia Inteventistica | Dr.Paolo Gazzo |

2012

S.C. Fisica Sanitaria

Ubicazione: piano terra pad. Vigiola presso l'ospedale San Paolo Via Genova, 30 Savona

Descrizione dei compiti istituzionali: 1)Supporto alle pratiche di radioterapia - elaborazione dello studio fisico dosimetrico, 2)Collaborazione con le SS.CC. di Radioterapia, Radiologia Diagnostica, Medicina Nucleare per la radioprotezione dei pazienti (D. Leg.vo 187/00); 3)Stesura di specifiche tecniche per l'acquisizione di apparecchiature di radiodiagnostica, radioterapia e medicina nucleare; 4)Stesura di specifiche tecniche, verifiche e collaudo di sistemi informatici utilizzati dalle SS.CC. Radiologiche del Dipartimento di Immagini; 5) effettuazione del controllo di qualità di apparecchiature di imaging non radiologico (ecografi); 6)Effettuazione dei controlli di sicurezza delle apparecchiature laser; 7) Sicurezza e controllo di qualità in materia di radiazioni non ionizzanti in genere; 8) Consulenze alle SS.CC aziendali in materia di fisica applicata alla medicina e biostatistica; 9) Attivita' di didattica nel campo della Fisica Medica e della Radioprotezione, 10) Compiti accessori – Radioprotezione del personale.NB: solo i compiti indicati ai punti 1, 2 e 10 implicano la gestione di dati personali

Trattamenti dati effettuati: 1) gestione banca dati pazienti avviati alla radioterapia 2)gestione banca dati pazienti che hanno effettuato esami rx e per cui e' necessario conoscere la dose assorbita 3)gestione banca dati dipendenti esposti a radiazioni 4)banca dati letture dosimetriche

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|--|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Int. | Est. |
| FIS SV 001 | gest.banca dati pazienti radioterapia | pazienti e utenti | x | | x | |
| FIS SV 002 | gest banca dati pazienti/utenti per dose assorbita | degenti e utenti | x | | x | |
| FIS SV 003 | gest. banca dati dipendenti esposti | dipendenti | x | | x | |
| FIS SV 004 | banca dati letture dosimetriche | dipendenti | x | | | x |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|--------------------------------|------------|-----------|-------------------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| FIS SV 001A | x | | Fisica San e Radioter | | | |
| FIS SV 001B | | x | Server Fisica Sanitaria | theraplan-plato | | x |
| FIS SV 002A | x | | Fisica Sanitaria | | | |
| FIS SV 002B | | x | Server Fisica Sanitaria | word | | |
| FIS SV 003A | x | | Fisica San. – Med. prev | | | |
| FIS SV 003B | | x | Server Fisica Sanitaria | access | | |
| FIS SV 004A | x | | sede Tecnorad | | | |
| FIS SV 004B | | x | | software dedicato | x | |

TABELLA 3 - Analisi dei rischi potenziali

| Rischi potenziali | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|--|----|----|---|-------|-------|
| | | | alta | media | bassa |
| | | | 1. Comportamenti degli operatori | | |
| a) Sottrazione di credenziali di autenticazione | | x | | | |
| b) Carenza di consapevolezza, disattenzione o incuria | | x | | | |
| c) Comportamenti sleali o fraudolenti | | x | | | |
| d) Errore materiale | x | | | | x |
| e) Altro: | | | | | |
| 2. Eventi relativi agli strumenti | | | | | |
| a) Azione di virus informatici o di programmi suscettibili di recare danno | x | | x | | |
| b) Spamming o tecniche di sabotaggio | | x | | | |
| c) Malfunzionamento, indisponibilità o degrado degli strumenti | x | | x | | |
| d) Accessi esterni non autorizzati | | x | | | |
| e) Intercettazione di informazioni in rete | | x | | | |
| f) Altro: | | | | | |
| 3. Altri Eventi | | | | | |
| a) Accessi non autorizzati a locali e/o reparti ad accesso ristretto | x | | x | | |
| b) Asportazione e furto di strumenti contenenti dati | x | | x | | |
| c) Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, condiz. ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | x | |
| d) Guasto ai sistemi complementari (imp. elettrico, climatizz) | x | | | x | |
| e) Errori umani nella gestione fisica della sicurezza | | x | | | |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|--------------------------------|------------------------------|---|---------------------------------------|
| da FIS SV 001A a FIS SV 003A | 1d; 3a,3b,3c | controllo correttezza dei dati restrizioni all'ingresso | videosorveglianza locali |
| da FIS SV 001B a FIS SV 003B | 1d; 2a,2c 3a 3b, 3c 3d | controllo correttezza dei dati, antivirus, backup, password, restrizioni all'ingresso | |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|-----------------------------------|-------------------------------|------------|----------------------------|-----------------|----------------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società esterna | Persona | |
| da FIS SV 001A a FIS SV 003A | copia | | x | | | personale s.c. | 12 ore |
| da FIS SV 001B a FIS SV 003B | backup periodico | x | x (dischi) | | | | 30 min |

TABELLA 7 – Trattamento dati affidato all'esterno

| Identificativo del trattamento | Soggetto esterno | Titolare | Responsabile | Impegno contrattuale all'adozione delle misure di sicurezza | |
|--------------------------------|------------------|---------------|---|---|----|
| | | | | SI | NO |
| FIS SV 004 A e B | Tecnorad-Verona | Soc. Tecnorad | Legale Rappresentante della soc. Tecnorad | x | |

S.C. Medicina Nucleare

Ubicazione: primo pad. chirurgico piano terra. ospedale Santa Corona Via xxv Aprile, 128 Pietra Ligure

Descrizione dei compiti istituzionali: prestazioni di diagnostica ambulatoriale, ricovero, terapia radiometabolica e diagnostica in laboratorio R.I.A.

Trattamenti dati effettuati: 1) gestione cartelle cliniche, 2) gestione referti

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|---------------------------------------|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Int. | Est. |
| MEN PL 001 | gestione cartelle cliniche | degenti | x | | x | |
| MEN PL 002 | gestione referti | degenti /utenti | x | | x | |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|--------------------------------|------------|-----------|------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| MEN PL 001 A | x | | reparto | | | |
| MEN PL 001 B | | x | server | software dedicato | | x |
| MEN PL 002 A | x | | reparto | | | |
| MEN PL 002 B | | x | server | software dedicato | | x |

TABELLA 3 - Analisi dei rischi potenziali

| | Rischi potenziali | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|--------------------------------------|--|----|----|---|-------|-------|
| | | | | alta | media | bassa |
| 1. Comportamenti degli operatori | a) Sottrazione di credenziali di autenticazione | x | | | x | |
| | b) Carenza di consapevolezza, disattenzione o incuria | x | | x | | |
| | c) Comportamenti sleali o fraudolenti | x | | | x | |
| | d) Errore materiale | x | | | x | |
| | e) Altro: | | x | | | |
| 2. Eventi relativi agli strumenti | a) Azione di virus informatici o di programmi suscettibili di recare danno | x | | | | x |
| | b) Spamming o tecniche di sabotaggio | x | | | x | |
| | c) Malfunzionamento, indisponibilità o degrado degli strumenti | x | | x | | |
| | d) Accessi esterni non autorizzati | x | | | | x |
| | e) Intercettazione di informazioni in rete | x | | | | x |
| | f) Altro: | | x | | | |
| 3. Altri Eventi | a) Accessi non autorizzati a locali e/o reparti ad accesso ristretto | x | | | x | |
| | b) Asportazione e furto di strumenti contenenti dati | x | | | | x |
| | c) Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, condiz. ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | | x |
| | d) Guasto ai sistemi complementari (imp. elettrico, climatizzazione) | x | | | | x |
| | e) Errori umani nella gestione fisica della sicurezza | x | | | x | |
| | f) Altro: | | x | | | |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|--------------------------------|--------------------|--|---------------------------------------|
| MEN PL 001 A MEN PL 002 A | 1 b | attività di formazione continua | |
| MEN PL 001 B MEN PL 002 B | 2 c | piattaforma di back.up, software di gestione app. rete, software di gestione remota, piano disaster/recovery | |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|-----------------------------------|-------------------------------|----------|----------------------------|-----------------|------------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società Esterna | Persona | |
| MEN PL 001 A | archiviazione | | X | | | | |
| MEN PL 001B | back-up su hardware esterni | X | | | | incaricato | |
| MEN PL 002B | | | | | | | 1 giono |

S.C. Neuroradiologia Diagnostica ed Interventistica Pietra Ligure

Ubicazione: piano terra del Pad. "Piastra dei Servizi" ospedale Santa Corona Via xxv Aprile, 128 Pietra Ligure

Descrizione dei compiti istituzionali: diagnostica e terapia del cranio e della colonna vertebrale

Trattamenti dati effettuati: 1)refertazione, 2)gestione banche dati degenti ed utenti 3)gestione dati a fini statistici ed amministrativi

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|---------------------------------------|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Inf. | Est. |
| NER PL 001 | refertazione | utenti/degenti | x | | x | |
| NER PL 002 | gest. banche dati degenti ed utenti | utenti/degenti | x | | x | |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|--------------------------------|------------|-----------|------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| NER PL 001A | x | | reparto | | | |
| NER PL 001B | | x | server | software dedicato | | x |
| NER PL 002 A | x | | reparto | | | |
| NER PL 002B | | x | server | software dedicato | | x |

TABELLA 3 - Analisi dei rischi potenziali

| | Rischi potenziali | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|--------------------------------------|--|----|----|---|-------|-------|
| | | | | alta | media | bassa |
| | | | | | | |
| 1. Comportamenti degli operatori | a) Sottrazione di credenziali di autenticazione | | x | | | |
| | b) Carenza di consapevolezza, disattenzione o incuria | | x | | | |
| | c) Comportamenti sleali o fraudolenti | | x | | | |
| | d) Errore materiale | x | | | x | |
| | e) Altro: | | | | | |
| 2. Eventi relativi agli strumenti | a) Azione di virus informatici o di programmi suscettibili di recare danno | | x | | | |
| | b) Spamming o tecniche di sabotaggio | | x | | | |
| | c) Malfunzionamento, indisponibilità o degrado degli strumenti | x | | | | x |
| | d) Accessi esterni non autorizzati | | x | | | |
| | e) Intercettazione di informazioni in rete | | x | | | |
| | f) Altro: | | | | | |
| 3. Altri Eventi | a) Accessi non autorizzati a locali e/o reparti ad accesso ristretto | | x | | | |
| | b) Asportazione e furto di strumenti contenenti dati | | x | | | |
| | c) Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, condiz. ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | x | |
| | d) Guasto ai sistemi complementari (imp. elettrico, climatizzazione) | x | | | x | |
| | e) Errori umani nella gestione fisica della sicurezza | x | | | | x |
| | f) Altro: | | | | | |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|--------------------------------|--------------------|---------------------------------|---|
| NER PL 001A NER PL 002A | 1 d | Sensibilizzazione del personale | aggiornamenti ,linee guida e protocolli operativi |
| NER PL 001B NER PL 002B | 2c | Password personale antivirus | |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|-----------------------------------|-------------------------------|----------|----------------------------|-----------------|---------------------------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società Esterna | Persona | |
| NER PL 001B NER PL 002B | back-up automatico | x | | | x | Amministratore di sistema | Tempo reale |
| NER PL 001B NER PL 002B | back-up su supporto magnetico | | x | | x | | |

S.C. Radiologia Diagnostica Albenga

Ubicazione: piano terra, lato ovest ospedale Santa Maria della Misericordia Viale Martiri della Foce 40, Albenga

Descrizione dei compiti istituzionali: diagnostica per Immagini (radiologia , TAC, ecografia , mammografia, risonanza magnetica)

Trattamenti dati effettuati: 1) consultazione e gestione banche dati degenti ed utenti per esami di diagnostica, 2) gestione banche dati esami di diagnostica 3) gestione refertazioni, 4) gestione banche dati a fini amministrativi, 5) gestione personale di reparto.

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|---|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Int. | Est. |
| RAD AL 001 | consultazione e gestione banche dati degenti ed utenti per esami di diagnostica | utenti/degenti | x | | x | |
| RAD AL 002 | gestione banche dati esami di diagnostica | utenti/degenti | x | | x | x |
| RAD AL 003 | gestione refertazioni | utenti/degenti | x | | x | |
| RAD AL 004 | gestione banche dati degenti ed utenti a fini amministrativi, | utenti/degenti | x | | x | |
| RAD AL 005 | gestione personale di reparto | dipendenti | x | | x | |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|--------------------------------|------------|-----------|-----------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| da RAD AL 001A a RAD AL 005A | x | | segreteria | | | |
| da RAD AL 001B a RAD AL 004B | | x | server dedicato | polaris | | x |
| RAD AL 005B | | x | segreteria | software dedicato | | |

TABELLA 3 - Analisi dei rischi potenziali

| Rischi potenziali | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|-----------------------------------|--|----|---|-------|-------|
| | | | alta | media | bassa |
| | | | | | |
| 1. Comportamenti degli operatori | a) Sottrazione di credenziali di autenticazione | | x | | |
| | b) Carenza di consapevolezza, disattenzione o incuria | x | | x | |
| | c) Comportamenti sleali o fraudolenti | | x | | |
| | d) Errore materiale | x | | | x |
| | e) Altro: | | | | |
| 2. Eventi relativi agli strumenti | a) Azione di virus informatici o di programmi suscettibili di recare danno | x | | | x |
| | b) Spamming o tecniche di sabotaggio | | x | | |
| | c) Malfunzionamento, indisponibilità o degrado degli strumenti | | x | | |
| | d) Accessi esterni non autorizzati | x | | | x |
| | e) Intercettazione di informazioni in rete | | x | | |
| | f) Altro: | | | | |
| 3. Altri Eventi | a) Accessi non autorizzati a locali e/o reparti ad accesso ristretto | x | | x | |
| | b) Asportazione e furto di strumenti contenenti dati | | x | | |
| | c) Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, condiz. ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | x |
| | d) Guasto ai sistemi complementari (imp. elettrico, climatizzazioni) | x | | x | |
| | e) Errori umani nella gestione fisica della sicurezza | | x | | |
| | f) Altro: | | | | |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|--------------------------------|--------------------|---|---|
| da RAD AL 001A a RAD AL 005A | 1 d 3a | sensibilizzazione del personale locali ad accesso ristretto e contenitori chiusi a chiave | aggiornamento periodico |
| da RAD AL 001B a RAD AL 005B | 2a . 3d | password personale antivirus e antispamming aziendale gruppo elettrogeno ospedaliero non a regime | potenziamento antivirus e antispamming ottimizzazione celere del sistema elettrogeno ospedaliero ed eventuale integrazione con gruppi di continuità limitazione degli accessi ai dati per i soli pazienti in cura applicazione dei dispositivi informatici previsti per i dati supersensibili informatizzazione di infortativa e consenso una tantum |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|---------------------------------------|-------------------------------|----------|----------------------------|-----------------|---------------------------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società Esterna | Persona | |
| da RAD AL 001A a RAD AL 005A | fotoriproduzione | | x | | | personale di struttura | 1 giorno |
| da RAD AL 001B a RAD AL 004B | back.up automatico | x | | | x | | tempo reale |
| da RAD AL 001B a RAD AL 005B | back.up mensile su supporto magnetico | | x | | x | amministratore di sistema | 1 giorno |

S.C. Radiologia Diagnostica ed Interventistica Pietra Ligure

Ubicazione: piano terra del pad. "Piastra dei Servizi" ospedale Santa Corona Via xxv Aprile, 128 Pietra Ligure

Descrizione dei compiti istituzionali: Esecuzione di tutte le tipologie di indagini digitali con IMAGING, sia con Raggi X che Risonanza Magnetica, Tomografia Computerizzata.

Trattamenti dati effettuati: 1) gestione cartelle cliniche, refertazione, 2) gestione banche dati degenti ed utenti, 3) gestione banche dati a fini statistici e amministrativi.

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|---------------------------------------|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Inf. | Est. |
| RAD PL 001 | gestione cartelle cliniche | degenti | x | | x | |
| RAD PL 002 | refertazione | utenti/degenti | x | | x | |
| RAD PL 003 | gest. banche dati degenti ed utenti | utenti/degenti | x | | x | |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|------------------------------------|------------|-----------|-----------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| RAD PL 001 RAD PL 002A RAD PL 003A | x | | reparto | | | |
| RAD PL 002B RAD PL 003B | | x | server centrale | software dedicato | | x |

TABELLA 3 - Analisi dei rischi potenziali

| Rischi potenziali | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|-----------------------------------|--|----|---|-------|-------|
| | | | alta | media | bassa |
| | | | | | |
| 1. Comportamenti degli operatori | a) Sottrazione di credenziali di autenticazione | | x | | |
| | b) Carenza di consapevolezza, disattenzione o incuria | | x | | |
| | c) Comportamenti sleali o fraudolenti | | x | | |
| | d) Errore materiale | x | | | x |
| | e) Altro: | | | | |
| 2. Eventi relativi agli strumenti | a) Azione di virus informatici o di programmi suscettibili di recare danno | x | | | x |
| | b) Spamming o tecniche di sabotaggio | | x | | |
| | c) Malfunzionamento, indisponibilità o degrado degli strumenti | x | | | x |
| | d) Accessi esterni non autorizzati | | x | | |
| | e) Intercettazione di informazioni in rete | | x | | |
| | f) Altro: | | | | |
| 3. Altri Eventi | a) Accessi non autorizzati a locali e/o reparti ad accesso ristretto | | x | | |
| | b) Asportazione e furto di strumenti contenenti dati | | x | | |
| | c) Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, ondi. ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | x |
| | d) Guasto ai sistemi complementari (imp. elettrico, climatizzazione) | x | | | x |
| | e) Errori umani nella gestione fisica della sicurezza | x | | | x |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|------------------------------------|--------------------|---------------------------------|---|
| RAD PL 001 RAD PL 002A RAD PL 003A | 1 d | sensibilizzazione del personale | aggiornamenti, linee guida e protocolli operativi |
| RAD PL 002B RAD PL 003B | 2c | password personale antivirus | |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|--|-------------------------------|----------|----------------------------|-----------------|---------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società Esterna | Persona | |
| RAD PL 002B RAD PL 003B | back-up automatico e su supporto magnetico | x | | | x | | tempo reale |

S.C. Radiologia Diagnostica ed Interventistica Savona- Cairo

Ubicazione: piano terra ospedale San Paolo, Via Genova 30 Savona

Descrizione dei compiti istituzionali: Attività di diagnostica tramite immagini digitali (IMAGING), Raggi X, Risonanza Magnetica, Tomografia Assiale Computerizzata e Ultra Suoni.

Trattamenti dati effettuati: 1) consultazione e gestione banche dati degenti ed utenti per esami di diagnostica
2) gestione banche dati esami di diagnostica 3) gestione refertazioni, 4) gestione banche dati degenti ed utenti a fini amministrativi, 5) gestione personale di reparto.

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|--|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Int. | Est. |
| RAD SV 001 | consultazione e gest. banche dati degenti ed utenti per esami di diagnostica | utenti/degenti | x | | x | |
| RAD SV 002 | gestione banche dati esami di diagnostica | utenti/degenti | x | | x | |
| RAD SV 003 | gestione refertazioni | utenti/degenti | x | | x | |
| RAD SV 004 | gest. banche dati degenti- utenti a fini amministrativi, | utenti/degenti | x | | x | |
| RAD SV 005 | gestione personale di reparto | dipendenti | x | | x | |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|--------------------------------|------------|-----------|-----------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| da RAD SV 001A a RAD SV 005A | x | | segreteria | | | |
| da RAD SV 001B a RAD SV 004B | | x | server dedicato | POLARIS | | x |
| RAD SV 005B | | x | segreteria | Software dedicato | | |

TABELLA 3 - Analisi dei rischi potenziali

| Rischi potenziali | | | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|--------------------------------------|----|--|----|----|---|-------|-------|
| | | | | | alta | media | bassa |
| 1. Comportamenti degli operatori | a) | Sottrazione di credenziali di autenticazione | | x | | | |
| | b) | Carenza di consapevolezza, disattenzione o incuria | | x | | | |
| | c) | Comportamenti sleali o fraudolenti | | x | | | |
| | d) | Errore materiale | x | | | x | |
| | e) | Altro: | | | | | |
| 2. Eventi relativi agli strumenti | a) | Azione di virus informatici o di programmi suscettibili di recare danno | x | | | x | |
| | b) | Spamming o tecniche di sabotaggio | | x | | | |
| | c) | Malfunzionamento, indisponibilità o degrado degli strumenti | | x | | | |
| | d) | Accessi esterni non autorizzati | | x | | | |
| | e) | Intercettazione di informazioni in rete | | x | | | |
| | f) | Altro: | | | | | |
| 3. Altri Eventi | a) | Accessi non autorizzati a locali e/o reparti ad accesso ristretto | | x | | | |
| | b) | Asportazione e furto di strumenti contenenti dati | | x | | | |
| | c) | Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, condizioni ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | x | |
| | d) | Guasto ai sistemi complementari (impianto elettrico, climatizzazione) | x | | | x | |
| | e) | Errori umani nella gestione fisica della sicurezza | x | | | | x |
| | f) | Altro: | | | | | |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|--------------------------------|--------------------|---|---|
| da RAD SV 001A a RAD SV 005A | 1 d . 3a | sensibilizzazione del personale locali ad accesso ristretto e contenitori chiusi a chiave | aggiornamento periodico |
| da RAD SV 001B a RAD SV 005B | 2a . 3d | password personale antivirus e antispam aziendale | potenziamento antivirus e antispam limitazione degli accessi ai dati dei soli pazienti in cura applicazione dei dispositivi informatici previsti per i dati supersensibili informatizzazione di informativa e consenso al trattamento dati una tantum utilizzo sistematico di password riservate e personali da aggiornarsi ogni tre/sei mesi (in relazione ai dati trattati) |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|---------------------------------------|-------------------------------|----------|----------------------------|-----------------|---------------------------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società Esterna | Persona | |
| da RAD SV 001A a RAD SV 005A | fotoriproduzione | | x | | | personale di struttura | 1 g |
| da RAD SV 001B a RAD SV 004B | back.up automatico | x | | | x | | tempo reale |
| da RAD SV 001B a RAD SV 005B | back.up mensile su supporto magnetico | | x | | x | amministratore di sistema | 30 minuti |

S.C. Radioterapia Savona

Ubicazione: piano primo monoblocco ospedale San Paolo Via Genova 30, Savona

Descrizione dei compiti istituzionali: applicazione di programmi di cura radioterapica al fine di eradicare patologie tumorali, in regime ambulatoriale, in degenti ricoverati o utenti esterni.

Trattamenti dati effettuati: 1) gestione banche dati degenti ed utenti 2) gestione cartelle cliniche radioterapiche

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|--|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Int. | Est. |
| RAO SV 001 | gest. banche dati degenti ed utenti | degenti/utenti | x | | x | |
| RAO SV 002 | gest. cartelle cliniche radioterapiche | degenti/utenti | x | | x | |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|--------------------------------|------------|-----------|------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| RAO SV 001A | x | | reparto | | | |
| RAO SV 001B | | x | | programma dedicato | | x |
| RAO SV 002A | x | | reparto | | | |
| RAO SV 002B | | x | | programma dedicato | | x |

TABELLA 3 - Analisi dei rischi potenziali

| Rischi potenziali | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|-----------------------------------|--|----|---|-------|-------|
| | | | alta | media | bassa |
| 1. Comportamenti degli operatori | a) Sottrazione di credenziali di autenticazione | | x | | |
| | b) Carenza di consapevolezza, disattenzione o incuria | | x | | |
| | c) Comportamenti sleali o fraudolenti | | x | | |
| | d) Errore materiale | x | | | x |
| | e) Altro: | | | | |
| 2. Eventi relativi agli strumenti | a) Azione di virus informatici o di programmi suscettibili di recare danno | x | | | x |
| | b) Spamming o tecniche di sabotaggio | x | | | x |
| | c) Malfunzionamento, indisponibilità o degrado degli strumenti | x | | | x |
| | d) Accessi esterni non autorizzati | | x | | |
| | e) Intercettazione di informazioni in rete | | x | | |
| | f) Altro: | | | | |
| 3. Altri Eventi | a) Accessi non autorizzati a locali e/o reparti ad accesso ristretto | x | | | x |
| | b) Asportazione e furto di strumenti contenenti dati | x | | | x |
| | c) Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, condiz. ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | |
| | d) Guasto ai sistemi complementari (imp. elettrico, climatizz) | x | | | x |
| | e) Errori umani nella gestione fisica della sicurezza | x | | | x |
| | f) Altro: | | | | |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|--------------------------------|--------------------|----------------------|---------------------------------------|
| RAO SV 001A RAO SV 002A | | archivi | |
| RAO SV 001B RAO SV 002B | | antivirus, password, | |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|-----------------------------------|-------------------------------|----------|----------------------------|-----------------|---------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società esterna | Persona | |
| RAO SV 001A RAO SV 002A | duplicazione cartaceo | | x | x | | | tempo reale |
| RAO SV 001B RAO SV 002B | back.up magnetico | | x | x | | | |

S.S.D. Angiografia e Radiologia Interventistica Pietra Ligure

Ubicazione: piano terra del pad. "Piastra dei Servizi" ospedale Santa Corona Via xxv Aprile, 128 Pietra Ligure

Descrizione dei compiti istituzionali: esecuzione di esami radiologici invasivi condotti per via percutanea attraverso strutture canalicolari a fini diagnostici e terapeutici.

Trattamenti dati effettuati: 1) gestione cartelle cliniche, 2) refertazione, 3) gestione banche dati degenti ed utenti, 4) gestione banche dati a fini statistici e amministrativi.

TABELLA 1 - Elenco dei trattamenti aventi ad oggetto dati sensibili o giudiziari

| Identificativo del trattamento | Descrizione sintetica del trattamento | | Natura dei dati trattati | | Altre strutture che concorrono al trattamento | |
|--------------------------------|---------------------------------------|--------------------------|--------------------------|-------|---|------|
| | Attività svolta | Categorie di interessati | Sens. | Giud. | Int. | Est. |
| ARI PL 001 | gestione cartelle cliniche | degenti | x | | x | |
| ARI PL 002 | refertazione | utenti/degenti | x | | x | |
| ARI PL 003 | gest. banche dati degenti ed utenti | utenti/degenti | x | | x | |

TABELLA 2 - Strumenti utilizzati

| Identificativo del trattamento | Banca dati | | Ubicazione | Procedure Utilizzate (Nome Software) | Interconnessione | |
|------------------------------------|------------|-----------|-----------------|--------------------------------------|------------------|----------|
| | cartacea | magnetica | | | Internet | Intranet |
| ARI PL 001 ARI PL 002A ARI PL 003A | x | | reparto | | | |
| ARI PL 002B ARI PL 003B | | x | server centrale | software dedicato | | x |

TABELLA 3 - Analisi dei rischi potenziali

| Rischi potenziali | SI | NO | Impatto sulla sicurezza dei dati e gravità stimata: | | |
|-----------------------------------|--|----|---|-------|-------|
| | | | alta | media | bassa |
| 1. Comportamenti degli operatori | a) Sottrazione di credenziali di autenticazione | | x | | |
| | b) Carenza di consapevolezza, disattenzione o incuria | | x | | |
| | c) Comportamenti sleali o fraudolenti | | x | | |
| | d) Errore materiale | x | | | x |
| | e) Altro: | | | | |
| 2. Eventi relativi agli strumenti | a) Azione di virus informatici o di programmi suscettibili di recare danno | x | | | x |
| | b) Spamming o tecniche di sabotaggio | | x | | |
| | c) Malfunzionamento, indisponibilità o degrado degli strumenti | x | | | x |
| | d) Accessi esterni non autorizzati | | x | | |
| | e) Intercettazione di informazioni in rete | | x | | |
| | f) Altro: | | | | |
| 3. Altri Eventi | a) Accessi non autorizzati a locali e/o reparti ad accesso ristretto | | x | | |
| | b) Asportazione e furto di strumenti contenenti dati | | x | | |
| | c) Eventi distruttivi, naturali o artificiali (sismi, scariche atmosferiche, incendi, allagamenti, ondi. ambientali ecc.), dolosi, accidentali o dovuti ad incuria | x | | | x |
| | d) Guasto ai sistemi complementari (imp. elettrico, climatizzazione) | x | | | x |
| | e) Errori umani nella gestione fisica della sicurezza | x | | | |

TABELLA 4 - Misure di sicurezza adottate o proposte

| Identificativo del trattamento | Rischi individuati | Misure esistenti | Tipologia di misure che si propongono |
|------------------------------------|--------------------|---------------------------------|---|
| ARI PL 001 ARI PL 002A ARI PL 003A | 1 d | sensibilizzazione del personale | aggiornamenti, linee guida e protocolli operativi |
| ARI PL 002B ARI PL 003B | 2c | password personale antivirus | |

TABELLA 5 - Criteri e procedure per il salvataggio e tempi di ripristino dei dati

| Identificativo del trattamento | Procedure per il salvataggio dati | Luogo di custodia delle copie | | Incaricato del salvataggio | | | Tempi di ripristino dati |
|--------------------------------|--|-------------------------------|----------|----------------------------|-----------------|---------|--------------------------|
| | | Server | Archivio | Struttura Interna | Società Esterna | Persona | |
| ARI PL 002B ARI PL 003B | back-up automatico e su supporto magnetico | x | | | x | | tempo reale |

2012