Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Linee guida per la Dematerializzazione del Consenso Informato in ambito radiologico

Le linee guida per la dematerializzazione del consenso informato in ambito radiologico sono state curate da:

SIRM

Dott. Giorgio Benea
Direttore Dipartimento Radiologia Clinica
Diagnostica ed Interventistica
Azienda Ospedaliero-Universitaria di Ferrara

Dott.ssa Maria Antonietta Calvisi
Direttore Struttura Semplice- Radiologia
Azienda USL N°3 Ospedale S. Francesco, Nuoro

Dott. Carlo Alberto Cametti
Direttore Dipartimento Servizio di Radiologia Dipartimento di
Diagnostica per Immagini
ASL TO2 Torino Ospedale San G. Bosco

Dott.ssa Francesca Coppola
Medico Radiologo, Radiologia Malpighi,
Dipartimento di Medicina Diagnostica e della prevenzione, Policlinico
Universitario S Orsola Malpighi, Bologna

Dott.ssa Nicoletta Gandolfo
Direttore Dipartimento Diagnostica per Immagini- ASL3- Regione Liguria
SC Radiologia Ospedale Villa Scassi – Genova

Prof Roberto Grassi
Professore Ordinario, Dipartimento di internistica clinica e sperimentale
Magrassi
Università della Campania Luigi Vanvitelli, Napoli

Dott. Carmelo Privitera
Direttore Dipartimento U.O.C. di Radiologia Ospedale Vittorio Emanuele
Az. Ospedaliero-Universitaria" Policlinico Vittorio Emanuele" Catania, Italia.

Prof Daniele Regge
Professore Associato Università di Torino
Direttore dell'Unità di Radiologia dell'Istituto di Candiolo, Torino, Italia.

Dott.ssa Agatina Rizzo
Dirigente Medico Specialista Radiologia
Az. Ospedaliero-Universitaria" Policlinico Vittorio Emanuele" Catania, Italia.

Agenzia per l'Italia Digitale (AgID), Presidenza del Consiglio dei Ministri.

Ing. Chiara Basile
Area Trasformazione Digitale

Ing. Stefano Van Der Byl
Area Trasformazione Digitale

AZIENDE

Ing. Fabio Capra
Development Manager RIS presso EL.CO.

Ing. Caterina Gatti
Responsabile Marketing e Vendite – MEDAS

Ing. Irene Minetti,
Marketing, EBIT S.r.L presso Esaote Group

Ing. Andrea Ramone
Manager It-H

SOMMARIO

PREMESSA

La dematerializzazione è un processo che ha come obiettivo la creazione di un flusso di documenti digitali aventi pieno valore giuridico, che vada prima ad affiancare e poi, sul lungo periodo, a sostituire la normale documentazione cartacea negli archivi di qualunque attività pubblica o privata. In ospedale questa rivoluzione ha avuto inizio negli ultimi decenni del secolo scorso con lo sviluppo dei sistemi di archiviazione delle immagini mediche (PACS) e successivamente con la creazione e progressiva integrazione dei documenti clinici del singolo paziente in un unico sistema, il fascicolo sanitario elettronico (FSE). L'introduzione della ricetta elettronica in molte regioni italiane porterà nel giro di poco tempo all'eliminazione del corrispettivo documento cartaceo. La dematerializzazione del consenso informato (CI), documento che certifica che il paziente abbia ricevuto dal medico curante tutte le informazioni disponibili sulla propria salute e sulla propria malattia, avendo pertanto la possibilità di scegliere, in modo informato, se sottoporsi a una determinata terapia o esame diagnostico, rappresenta un ulteriore passo verso la completa dematerializzazione dei documenti prodotti in ambito sanitario. Il CI costituisce il fondamento della liceità dell'attività sanitaria, in assenza del quale l'attività stessa costituisce reato. In considerazione dell'importanza legale del documento, è sicuramente necessario strutturare un processo che definisca l'interazione medico/paziente in maniera conforme ai requisiti legislativi e tecnologici necessari per la sua implementazione.
La Società Italiana di Radiologia Medica (SIRM) ha promosso lo sviluppo delle linee guida per la dematerializzazione del consenso informato (DCI) contenute in questo documento, affidando la sua realizzazione alla Sezione di studio di Radiologia Informatica e alla Commissione Consenso Informato della società. Le linee guida oggetto della sperimentazione promossa dalla SIRM sono destinate sia all'ambito ospedaliero che all'ambito ambulatoriale, sia Pubblico che Privato in modo indistinto, così come indistinta è la Normativa a cui esse fanno riferimento. Fin dalle prime fasi il gruppo di lavoro ha invitato a far parte del progetto stakeholder industriali del settore IT i quali hanno aderito partecipando alla iniziale fase di sperimentazione clinica e contribuendo alla stesura delle sezioni ad elevato contenuto tecnologico. La sperimentazione clinica, a cui inizialmente hanno aderito 16 strutture di Radiodiagnostica e diverse aziende IT, aveva i seguenti obiettivi: 1. identificare le migliori soluzioni tecnologiche per l'implementazione della DCI; 2. sperimentare l'utilizzo della DCI in diversi ambiti radiologici; 3. misurare l'impatto della DCI sull'attività di un reparto di radiologia; 4. identificare vantaggi e svantaggi dell'applicazione della DCI sui flussi di lavoro radiologico. Ambiti di applicazione e soluzioni tecnologiche adottate sono elencate in modo sintetico limitatamente agli 8 centri che hanno portato a termine la sperimentazione nel "*Documento di sintesi della Sperimentazione - Dematerializzazione del Consenso Informato in ambito radiologico*".
Tutti i centri coinvolti nella sperimentazione hanno identificato e utilizzato per la firma del consenso informato e del questionario anamnestico per i pazienti lo strumento della firma elettronica avanzata (in particolare la soluzione di firma grafometrica) e per il medico dell'area radiologica lo strumento di firma elettronica qualificata. La sperimentazione ha quindi avuto esito positivo con buona adesione dei pazienti e disponibilità da parte del personale medico, tecnico e amministrativo a partecipare a tutte le fasi di realizzazione del progetto.
I vantaggi e gli svantaggi emersi nello studio sono elencati in dettaglio nel "*Documento di sintesi della Sperimentazione - Dematerializzazione del Consenso Informato in ambito radiologico*". Con la finalità di comprendere la propensione dei medici dell'area radiologica verso la dematerializzazione del CI i soci SIRM sono stati invitati a completare un questionario composto da 15 domande. Al sondaggio hanno aderito 1791 radiologi (18% del totale di iscritti SIRM) e la grande maggioranza dei rispondenti (95%) si è dimostrata favorevole al DCI. Inoltre nel "*Documento di sintesi della Sperimentazione - Dematerializzazione del Consenso Informato in ambito radiologico*" sono elencati i vantaggi e svantaggi del DCI secondo il parere dei medici dell'area radiologica rispondenti con relative percentuali.

La Figura 1 sottostante mostra un esempio di workflow dei passi necessari per l'erogazione di una prestazione radiologica.

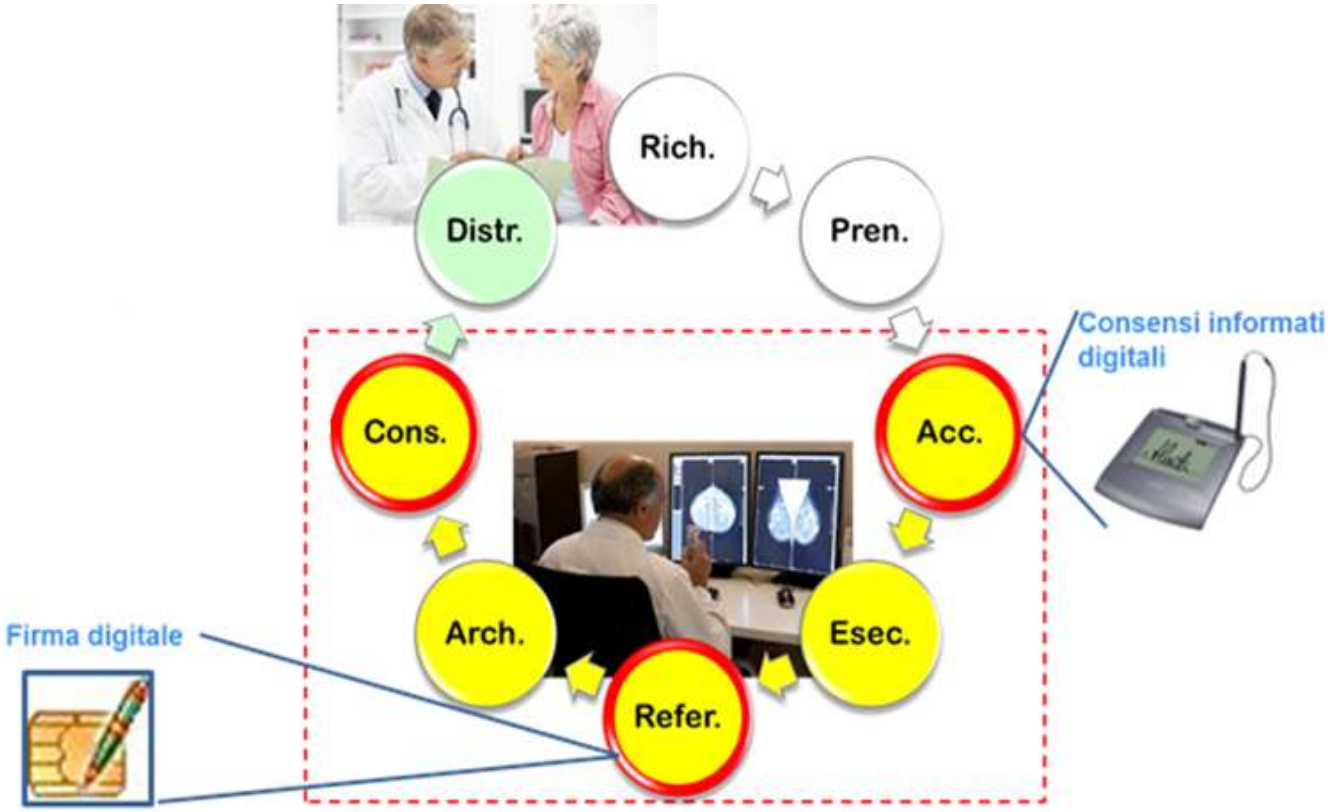

Figura 1 - Workflow prestazione radiologica

CONSENSO INFORMATO E DEMATERIALIZZAZIONE

Definizione e caratteristiche del consenso informato

Il consenso informato è un obbligo contrattuale e la violazione del dovere d'informazione dà luogo a precise responsabilità. In particolare la Convenzione di Oviedo **(Legge 145, 28 marzo 2001)** dedica alla definizione del consenso il capitolo 2, art. da 5 a 9, in cui stabilisce, come regola generale che *"un intervento, nel campo della salute, non può essere effettuato se non dopo che la persona interessata abbia dato consenso libero e informato. Questa persona riceve innanzitutto una informazione adeguata sullo scopo e sulla natura dell'intervento e sulle conseguenze e i suoi rischi. La persona interessata, può in qualsiasi momento, liberamente ritirare il proprio consenso.".* Inoltre il **Codice Penale, Art. 50** fa riferimento alla necessità di munirsi in via preventiva, del consenso del paziente *"non è punibile chi lede o pone in pericolo un diritto con il consenso della persona che può validamente disporne".*
Nel documento SIRM **"Atto medico Radiologico"** si afferma che il Consenso all'effettuazione dell'esame radiologico, giuridicamente valido, deve essere informato. L'informazione corretta e completa deve essere:

a) *Semplice*, perché il paziente non è esperto di medicina - personalizzata in base alla cultura e alla comprensione dell'assistito - esauriente, perché l'informazione deve esplicitare i rischi prevedibili - veritiera, ma emotivamente equilibrata.
b) *Esplicita.* Non può mai essere desunta o implicita ma deve rispettare le modalità previste. La forma scritta non è sempre obbligatoria ma è prova certa dell'avvenuta informazione e può rappresentare un momento utile di riflessione per il paziente.
c) *Libera*. Non è valida su coercizione o acquisito con inganno o errore.
d) *Personale.* Deve essere rilasciata esclusivamente dal diretto interessato, salvo eccezioni. Nel caso di minore o di soggetto malato di mente o incapace di intendere e di volere il consenso, per essere valido, dovrà essere prestato da chi ne esercita la potestà: i genitori o il tutore legalmente designato, ovvero il rappresentante legale (tutore o curatore) dell'incapace. Tuttavia i confini tra potestà e volontà dei minori sono molto labili: il minorenne ha diritto di essere informato e di esprimere i suoi desideri. Qualora sussista disaccordo tra la volontà dei genitori e il parere dei medici curanti, questi ultimi potranno presentare ricorso all'Autorità Giudiziaria.
e) *Consapevole e manifesta.* Ottenuta dopo un'informazione corretta e completa da paziente capace di intendere e di volere nel momento in cui viene espresso.
f) *Preventiva.* Deve precedere l'intervento sanitario restando suscettibile di revoca.
g) *Specifica.* Deve essere riferita unicamente alla prestazione, diagnostica e/o interventistica, che viene prospettata al paziente, salvo nei casi in cui si può configurare uno stato di necessità.

La dematerializzazione del consenso informato

La sottoscrizione al consenso può anche essere registrata dal medico con strumenti informatici secondo le attuali norme legislative (**D.P.C.M. 22/2/2013, G.U. n. 117 del 21/5/2013, art 55,56,57**). Si effettua in tal modo un processo di dematerializzazione che ha come obiettivo la creazione di documenti informatici aventi pieno valore giuridico, che vada prima ad affiancare e poi, sul lungo periodo, a sostituire la normale documentazione cartacea presente negli archivi. Come già evidenziato nel documento di sintesi della sperimentazione e nell'introduzione a questo documento, il processo di dematerializzazione ha una serie di vantaggi rappresentati in prima istanza

dall'incremento di efficienza e dalla riduzione dei costi. Inoltre consente di ovviare a diversi limiti della conservazione tradizionale: la difficoltà di condivisione, la facilità di smarrimenti e gli elevati tempi di ricerca sono alcuni degli esempi particolarmente rilevanti.
Nella tradizionale gestione della documentazione cartacea il valore giuridico del documento è rappresentato dalla firma autografa, ovvero la firma apposta di pugno da chiunque sottoscriva un documento. Essa è considerata un elemento distintivo aventi caratteristiche uniche e personali. La dematerializzazione permette di produrre documenti digitali con pieno valore giuridico e per questo è necessario adottare un sistema che consenta di accertare in maniera chiara ed univoca il sottoscrittore di un documento.
Il Codice dell'Amministrazione Digitale *(CAD)* introduce nel nostro ordinamento, in aggiunta alla *Firma Elettronica Qualificata,* nuove fattispecie di firma elettronica in grado di soddisfare il requisito fondamentale della riconducibilità della firma stessa al sottoscrittore fino a prova contraria. Tra queste, la *Firma Elettronica Avanzata (FEA)* apre la strada a nuove tecnologie che consentono l'uso del documento informatico, in luogo del tradizionale foglio cartaceo, in diversi contesti applicativi. In particolare, si autorizza l'uso di tecnologie biometriche, e quindi della Firma Grafometrica (FG), per l'acquisizione della *Firma Elettronica Avanzata*, consentendo l'efficace dematerializzazione anche di documenti firmati da soggetti non dotati di firma elettronica qualificata.
Il successivo DPCM del 22 febbraio 2013, completa e definisce, quindi, quanto introdotto dal Codice dell'Amministrazione Digitale, indicando, fra gli altri punti, anche le regole tecniche relative alla generazione, apposizione e verifica della Firma Elettronica Avanzata.
Una particolare tipologia di FEA, che soddisfa i requisiti del su citato DPCM è rappresentata dalla firma grafometrica. Essa è prodotta personalmente da un paziente, di proprio pugno, mediante l'impiego di un apposito hardware di acquisizione, come ad esempio speciali tavolette di acquisizione (tablet grafometrici), o anche su dispositivi tablet di uso generale equipaggiati con opportuni sensori e programmi software. I dispositivi di acquisizione utilizzati sono in grado di rilevare, oltre che il tratto grafico, anche una serie di parametri dinamici associati all'atto della firma (velocità di tracciamento, accelerazione, pressione, inclinazione, salti in volo …).
La firma così acquisita viene associata al documento informatico (in formato PDF) che riproduce il contenuto e lo rende visibile allo scopo di impedire l'alterazione del testo per la sua sottoscrizione.
La firma grafometrica, pertanto, offre da un lato la protezione dell'integrità del documento e la piena digitalizzazione/dematerializzazione al pari della firma elettronica qualificata, e dall'altro la semplicità e l'intuitività della firma autografa.

In sintesi quindi, la FEA Grafometrica, una modalità di sottoscrizione di un documento informatico da parte di un soggetto opportunamente identificato mediante un valido documento di riconoscimento, è risultato la modalità più idonea per la sottoscrizione del consenso informato.
La FG, sul piano giuridico ha la stessa validità legale del documento cartaceo sottoscritto con firma autografa, anche ai fini probatori e pertanto ha l'efficacia prevista dall'art.2702 del Codice Civile.
Il documento informatico sottoscritto con FG è realizzato in modo tale che vengano garantite:

- l'identificazione del firmatario;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo in capo al soggetto sottoscrivente del sistema di generazione della firma;
- la connessione univoca della firma al documento sottoscritto;
- l'immodificabilità ed inalterabilità del documento sottoscritto;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- la connessione univoca della firma al documento sottoscritto.

Processo per l'acquisizione del consenso informato

Al fine di sottoscrivere il consenso informato alla prestazione radiologica con FEA, il paziente deve già aver rilasciato in precedenza il consenso all'utilizzo della firma grafometrica. In questo paragrafo vengono descritte le modalità di acquisizione del consenso informato sia nel caso in cui il paziente effettui il primo accesso alla struttura, sia nel caso abbia già prestato il consenso all'utilizzo della FG in precedenza.

Il primo passo da compiere, se non si è già acquisito in precedenza, è quello di raccogliere l'autorizzazione all'uso della FEA e al trattamento dei dati biometrici da parte del paziente:

- all'acceso del paziente nella struttura viene fatto il suo riconoscimento da parte di un operatore sanitario tramite verifica con documento di riconoscimento in corso di validità (ad es. carta d'identità, passaporto, etc.) ed inserimento/completamento in anagrafica del Sistema informativo Radiologico (RIS) come da DPCM 22 febbraio 2013 art. 57 co. 1 lettera a);
- se il paziente non è provvisto o si rifiuta di mostrare il documento d'identità egli non può sottoscrivere con lo strumento di FG e pertanto si adotta la modalità di firma su cartaceo;
- scansione del documento d'identità (DPCM 22 febbraio 2013 art. 57 co. 1 lettera b).
- visualizzazione e spiegazione dell'informativa relativa all'utilizzo della FEA (DPCM 22 febbraio 2013 art. 57 co. 1 lettera a);
- raccolta dell'autorizzazione all'uso della FEA e al trattamento dei dati biometrici, tramite autorizzazione orale e sottoscritto tramite firma digitale remota (DPCM 22 febbraio 2013 art 57 co. 5);
- possibilità di fornire al richiedente copia dell'adesione all'uso della FEA.

Una volta acquisito il consenso all'uso della FEA, il medico dell'area radiologica potrà procedere alla prestazione di diagnostica per immagini con l'acquisizione del consenso informato, ovvero:

- Anamnesi, giustificazione e completamento della spiegazione della procedura diagnostica da parte del medico dell'area radiologica dopo che il paziente ha preso visione sia dell'informativa sulla prestazione diagnostica sia all'informativa relativa al trattamento dei dati personali;
- Compilazione, di concerto con il paziente, del Questionario Anamnestico;
- Sottoscrizione del documento informatico comprensivo del questionario anamnestico e del Consenso Informato alla prestazione di diagnostica per immagini da parte del medico radiologo dell'area radiologica attraverso la firma qualificata;
- Sottoscrizione del documento informato comprensivo del questionario anamnestico e del Consenso Informato alla prestazione di diagnostica per immagini da parte del paziente attraverso la firma grafometrica;
- Conferma e chiusura dell'iter da parte del medico dell'area radiologica attraverso la sottoscrizione del consenso informato con Firma elettronica qualificata.

La raccolta del CI deve essere quindi effettuata da uno dei medici dell'area radiologica che partecipa alla conduzione dell'esame. L'approvazione fornita dal paziente tramite sottoscrizione del CI potrà essere revocata in qualsiasi momento sino all'effettiva esecuzione dell'esame in conformità al DPCM 22 febbraio 2013 art. 57 co. 1 lettera h).

In caso di pazienti impossibilitati a muoversi in quanto allettati, con disabilità o collegati ad apparecchiature di monitoraggio, è importante sottolineare che il consenso può essere sottoscritto

anche da dispositivi di acquisizione di tipo tablet, purché dotati di una superficie in grado di acquisire i parametri biometrici del firmatario.
Il risultato del processo sopra descritto è un documento digitale di consenso informato sottoscritto con firma grafometrica da parte del paziente e di firma elettronica qualificata da parte dell'operatore sanitario. Il documento informatico di consenso può anche essere strutturato, ad esempio con standard CDA2, per una sua successiva elaborazione.

La Figura 2 di seguito illustra il diagramma di flusso del processo di acquisizione del consenso informato:

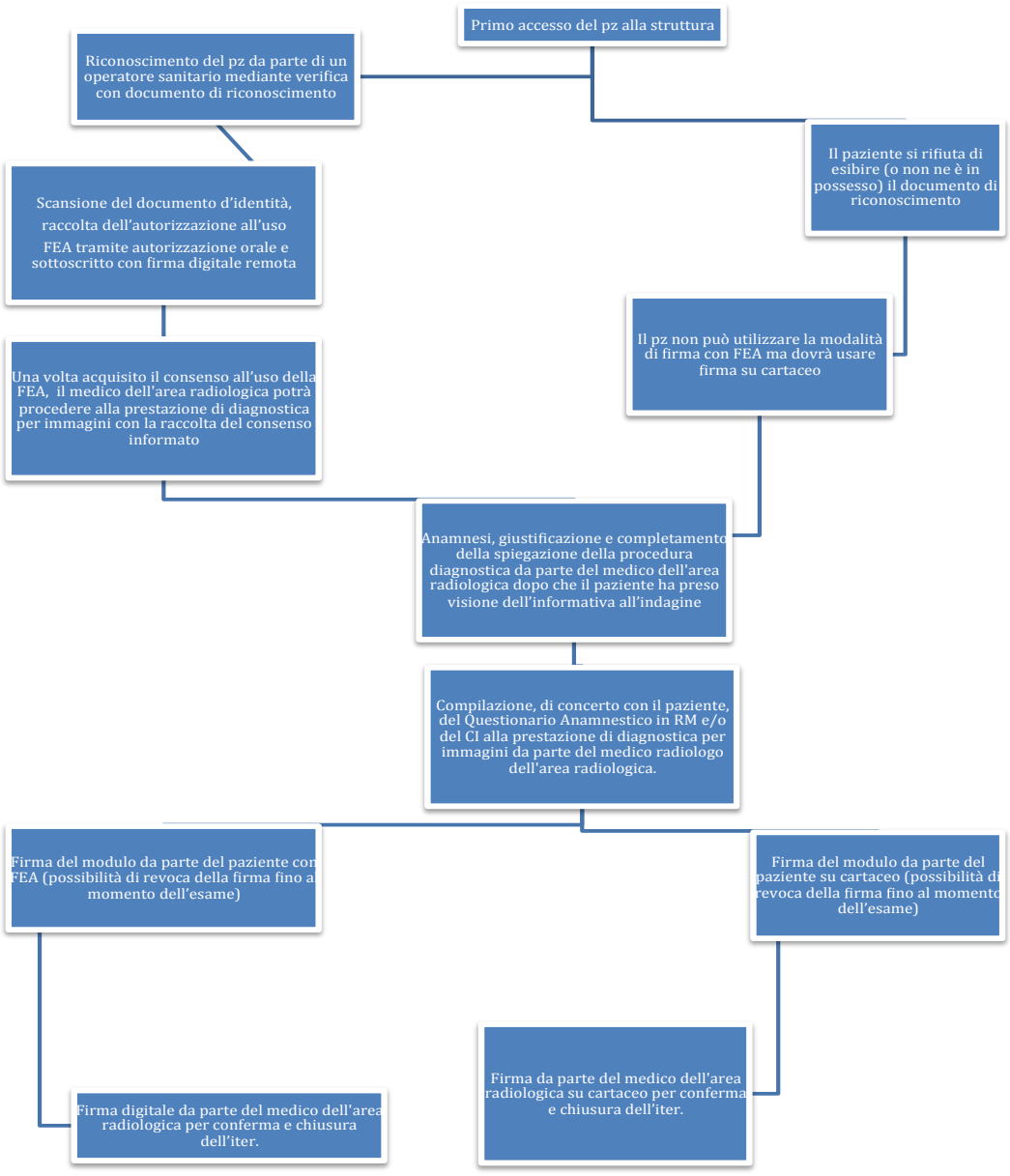

Figura 2 - Diagramma di flusso del processo di acquisizione del consenso informato

Trattamento dei dati biometrici nel processo di dematerializzazione del consenso informato

Il trattamento di dati biometrici per scopi di autenticazione informatica, di controllo degli accessi e di sottoscrizione di documenti informatici deve essere svolto in conformità a quanto previsto dal "**Provvedimento generale prescrittivo del Garante per la Protezione dei Dati Personali del 12 novembre 2014".**

Nell'Allegato A viene fornito un dettaglio di analisi di conformità del processo al citato provvedimento.

Il personale coinvolto nella gestione del consenso informato

Risulta peraltro importante sintetizzare correttamente le diverse fasi del processo in relazione agli operatori interessati nell'acquisizione del consenso informato.
Nel processo sono identificate tre figure professionali coinvolte nell'acquisizione del consenso informato: il personale amministrativo, il personale sanitario non medico, solitamente i tecnici sanitari di radiologica medica (TSRM) e gli infermieri professionali (IP) e il personale sanitario medico.
La prima fase prevede l'identificazione del paziente e l'acquisizione del consenso all'uso della firma grafometrica e al trattamento dei dati biometrici. In questa fase solitamente il personale coinvolto è il personale amministrativo:

- ***Il personale amministrativo*** può essere incaricato dell'acquisizione del consenso all'uso della FG: questo personale svolge già l'identificazione del Paziente ed è addetto alla verifica dei dati anagrafiche. Va sottolineato che la raccolta di questo consenso avviene "una tantum".

La seconda fase prevede l'acquisizione del consenso informato da parte degli operatori sanitari, che comprende l'acquisizione del consenso al trattamento dei dati personali e l'acquisizione al consenso a sottoporsi all'indagine di diagnostica per immagini.
In questa fase sono coinvolti sia il personale sanitario non medico sia il personale sanitario medico, ed in particolare:

- ***Il personale sanitario non medico,*** delegabile per gli aspetti pratici delle procedure, accoglie il paziente in sala d'attesa. Tale figura professionale è designata per consegnare al paziente il testo dell'informativa e il testo del consenso alla indagine di diagnostica per immagini in formato cartaceo o invitare il paziente a prenderne visione di tale documentazione qualora sia consultabile attraverso altri dispositivi (ad es. visualizzato su monitor a parete negli spazi di attesa, consultabile sul sito aziendale, etc.).

- ***Il personale medico radiologico*** è deputato all'acquisizione del consenso informato del paziente attraverso la sottoscrizione del documento digitale tramite apposizione della firma grafometrica del paziente e della sua sottoscrizione con firma elettronica qualificata in fase di avvio e di chiusura del processo.

CONTESTO NORMATIVO

Principali testi normativi

Nel seguito del presente paragrafo verrà presentata una panoramica generale della normativa vigente, applicata al processo di dematerializzazione dei consensi informati, oggetto di queste linee guida.

Sono di seguito riportati, in ordine cronologico, i riferimenti ai principali testi normativi relativi alla corretta gestione dei consensi informati digitali e all'utilizzo della firma grafometrica che, se risponde ai requisiti previsti dalla norma, costituisce una tipologia di firma elettronica avanzata.

Normativa europea

Norma	**Breve descrizione**
Regolamento Europeo n. 910/2014 – eIDAS	Il regolamento dispone le condizioni dei prestatori di servizi fiduciari tra cui rientrano attività come il rilascio di firme elettroniche e marche temporali. Il regolamento abroga la precedente direttiva europea 93/1999 che è stata alla base della normativa sulle firme in tutti gli stati membri.
Regolamento Europeo n. 679/2016 - Nuovo regolamento privacy.	Il regolamento dispone le condizioni di trattamento dei dati personali di persone fisiche alle quali gli stati membri dovranno adeguarsi entro il termine di due anni. Il regolamento abroga la precedente direttiva 95/46/CE (Regolamento sulla protezione dei dati).

Tabella 1 - Normativa Europea

Normativa nazionale

Norma	**Breve descrizione**
D.P.R. 445/2000 – Testo unico sulla documentazione amministrativa	Riferimento alle sezioni riguardanti i documenti informatici.
D. lgs. 196/2003 – Codice in materia di protezione dei dati personali	Anche la FEA ed il correlato processo di implementazione ed uso, data la loro natura, devono sottostare alla normativa in oggetto (successivamente a questo D. Lgs il garante ha emesso delle linee guida che chiariscono e schematizzano gli ambiti di implementazione ed utilizzo).
D. lgs. 82/2005 – Codice dell'amministrazione digitale e s.m.i.	È la principale normativa di riferimento in ambito di amministrazione digitale.

Norma	Breve descrizione
D. lgs 235/2010 – Modifiche ed integrazioni al decreto legislativo 7 Marzo 2005 n. 82 recante codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69	È il D. Lgs che, integrando il D. lgs. 82/2005, definisce la FEA e la firma grafometrica. Il documento rimanda, quindi, a regole tecniche di diversa natura successivamente emesse, che definiscono i dettagli anche della procedura di implementazione ed utilizzo.
D.P.C.M. 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2 e 71.	È il principale documento di riferimento che regola i dettagli e gli ambiti di implementazione ed utilizzo per la firme elettroniche avanzate, qualificate e digitali.
D.P.C.M. 03 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57 –bis e 71, del codice dell'amministrazione digitale di cui al decreto legislativo n° 82 del 2005.	Regole tecniche per la gestione del protocollo informatico.
Provvedimento prescrittivo n.513 del Garante della Privacy del 12 novembre 2014	Provvedimento generale prescrittivo in tema di biometria in particolare Allegato A "Linee guida in tema di riconoscimento biometrico e firma grafometrica"; Allegato B "Modulo di segnalazione data breach".
13 novembre 2014 – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.	Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni.
D. lgs 179/2016 - Modifiche ed integrazioni al codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n.82.	E' il D. lgs che, integrando e in parte modificando il D. lgs 82/2005, riconosce nuovo valore giuridico alla firma elettronica semplice (alla quale viene riconosciuto il requisito della forma scritta, pur rimanendo liberamente valutabile in sede di giudizio).

Tabella 2 - Normativa Nazionale

GLOSSARIO E DEFINIZIONI

Acronimo	Definizione
AgID	Agenzia per l'Italia Digitale.
CA	Certification Authority – Autorità di Certificazione.
CAD	Codice dell'Amministrazione Digitale, Decreto Legislativo 7 marzo 2005, nr. 82.
Certificati Elettronici	Gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche.
Certificato Qualificato	Attestato elettronico mediante il quale il fornitore dei servizi di certificazione (certificatore) dichiara di avere identificato il titolare del dispositivo di firma o degli strumenti per l'accesso al servizio di firma remota e di averglieli consegnati, in conformità con quanto definito nell'Art 28 commi 1-2 del codice per l'amministrazione digitale.
Certificatore	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime.
Chiave Privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave Pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.
Consenso Informato (CI)	Forma di autorizzazione del paziente a ricevere un trattamento sanitario, medico o infermieristico, previa la necessaria informazione sul caso da parte del personale sanitario proponente: il paziente ha il diritto/dovere di conoscere tutte le informazioni disponibili sulla propria salute e la propria malattia, potendo chiedere al medico tutto ciò che non è chiaro, avendo pertanto la possibilità di scegliere, in modo informato, se sottoporsi a una determinata terapia o esame diagnostico. Tale consenso costituisce il fondamento della liceità dell'attività sanitaria, in assenza del quale l'attività stessa costituisce reato. Il fine della richiesta del consenso informato è dunque quello di promuovere l'autonomia o libertà di scelta dell'individuo nell'ambito delle decisioni mediche.

Dati biometrici	Pur non esistendo, allo stato, una definizione normativa concernente i "dati biometrici", questi vengono convenzionalmente definiti come dati ricavati da "proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità". Per esigenze di armonizzazione dei termini usati in un contesto caratterizzato da notevole tecnicismo, si ritiene tuttavia necessario utilizzare le definizioni fornite dallo standard internazionale ISO/IEC 2382-37 "Information Technology — Vocabulary — Part 37: Biometrics".
DCI	Consenso informato dematerializzato
Dematerializzazione	Processo che ha come obiettivo ultimo la creazione di un flusso di documenti digitali aventi pieno valore giuridico, che vada prima ad affiancare e poi, sul lungo periodo, a sostituire la normale documentazione cartacea presente negli archivi di qualunque attività pubblica o privata.
Dispositivo di firma	Strumento ad elevata sicurezza, che contiene la chiave privata in esclusivo possesso del titolare. Si tratta di una smartcard o di una chiavetta USB, a cui vanno aggiungendosi recentemente i servizi di firma remota basati su server centralizzati che ospitano le chiavi di molti utenti.
Firma autografa	La firma che un soggetto appone di suo pugno su un documento, avendo essa elementi distintivi e caratteristiche uniche, al fine di assumere la paternità della dichiarazione in esso contenuta.
Firma digitale (FD)	La firma digitale è un particolare tipo di firma elettronica avanzata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Firma Elettronica (FE)	La firma elettronica come "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica";
Firma Elettronica Avanzata (FEA)	La firma elettronica avanzata come insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma Elettronica Qualificata (FEQ)	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

Firma Grafometrica (FG)	E' un particolare tipo di firma elettronica avanzata che si ottiene dal rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, movimento e via dicendo) della firma di un individuo che utilizza una penna elettronica per scrivere su una tavoletta (tablet) biometrica, cioè dotata di particolari sensori atti al recepimento dei suddetti dati calligrafici.
FSE	Fascicolo sanitario elettronico
IP	Infermiere Professionale
IT	Information Tecnology
MPK	Master Protection Key – Chiave di cifratura dei dati biometrici
PACS	Picture archiving and communication system
Parametri Grafometrici	Un insieme di parametri (posizione, pressione, tempo da cui è possibile derivare velocità, pressione, ritmo, accelerazione, movimenti aerei) che vengono "catturati" nel momento in cui si appone una firma autografa su una particolare dispositivo (generalmente tablet) e che rendono certa l'autenticazione del Titolare.
RIS	Il Radiology Information System è il sistema informatico utilizzato nelle Radiologie per gestire il flusso dei dati legati ai pazienti.
Software di firma	Sistema che sia in grado di operare e gestire il dispositivo di firma e di produrre documenti firmati digitalmente, mediante la chiave privata, completi di una copia del certificato qualificato, il quale consentirà di verificare la firma e accertare così l'identità del sottoscrittore del documento.
Tablet di firma	Tavoletta (tablet) biometrica dotata di "penna elettronica" in grado di rilevare il tratto e i dati calligrafici della firma.
Titolare	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
TSRM	Tecnico Sanitario di Radiologia Medica.

Tabella 3 - Glossario e definizioni

ALLEGATO A

REQUISITI NORMATIVI E TECNOLOGICI PER LA DEMATERIALIZZAZIONE DEL CONSENSO INFORMATO

Introduzione

Come stabilisce la normativa vigente, è necessario che il fornitore del sistema di firma elettronica avanzata, fornisca nel modo più trasparente possibile, ossia attraverso la pubblicazione sul sito web della struttura che eroga il servizio, la descrizione delle caratteristiche del sistema e delle tecnologie utilizzate al fine di garantire l'ottemperanza a quanto prevede la normativa in termini di Caratteristiche Tecniche per la Firma Elettronica Avanzata (DPCM 22.02.2013, art. 56).
Oltre a ciò, se la soluzione di firma è declinata nella sua specificità grafometrica, il soggetto erogatore del servizio deve tenere in considerazione anche il provvedimento generale prescrittivo in tema di biometria del Garante stesso del 12 novembre 2014: esso prevede per alcune casistiche di trattamento dei dati personali (come nella fattispecie il trattamento dei dati biometrici nell'ambito della sottoscrizione di documenti informatici), la possibilità di essere esonerato dalla verifica preliminare da parte del Garante per la Protezione dei dati personali (di cui all'art. 17 del D.lgs. 196/2003, Codice della Privacy). Per evitare questa operazione di verifica preliminare, il Titolare del Trattamento dei dati personali della struttura che eroga il servizio di firma deve rispettare un elenco di prescrizioni e limitazioni definito all'interno del presente provvedimento.
Dal momento che le dette prescrizioni e limitazioni riguardano in parte aspetti tecnologici e in parte aspetti organizzativi è necessario che i soggetti coinvolti siano allineati e consapevoli ciascuno delle proprie responsabilità. Le parti che descrivono gli aspetti tecnologici della soluzione di fatto trattano le stesse informazioni che il DPCM 22.02.2013 (art. 57, comma 1) prevede siano pubblicate sul sito web della struttura erogante.
Il presente capitolo descrive le evidenze che consentono all'azienda sanitaria di essere esonerata dall'obbligo di presentare istanza di verifica preliminare al Garante per la protezione dei dati personali relativamente all'uso del servizio di firma grafometrica per la sottoscrizione di alcuni documenti informatici prodotti all'interno dell'azienda sanitaria stessa. In particolare vengono qui illustrate le caratteristiche tecnologiche ed organizzative richieste dal suddetto "Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014" con particolare attenzione per l'art. 4.4 "Sottoscrizione di documenti informatici" relativamente all'apposizione di FG e firma digitale.

Caratteristiche del software per la sottoscrizione del documento informatico tramite firma grafometrica

Il software utilizzato nel processo di acquisizione della firma elettronica avanzate con l'acquisizione di dati biometrici grafometrica deve essere in grado di gestire anche la firma elettronica qualificata.
Le applicazioni dell'azienda sanitaria che necessitano di apporre una firma grafometrica ad un documento informatico, lo inviano all'apposito applicativo che si occupa di tutte le fasi dell'acquisizione della firma. Questo software una volta acquisita la firma, invia all'applicazione chiamante un documento informatico contenente la firma grafometrica dell'interessato. Tale documento viene poi controfirmato con firma digitale dell'operatore che ha identificato il firmatario e raccolto la sua firma.

L'apposizione della firma grafometrica avviene tramite specifiche postazioni di lavoro sulle quali è installato il modulo software ed è connesso con il dispositivo hardware tablet che rende possibile l'acquisizione della FG stessa.
Tutte le postazioni di lavoro dovrebbero esser censite dalla società fornitrice della soluzione di firma e su di esse viene fatto l'enrollment in modo protetto del certificato pubblico con cui sono cifrati i dati biometrici.

Caratteristiche della firma grafometrica

Come già definito nelle linee guida, la FG è il risultato di una procedura che consiste nell'uso di tecniche biometriche basate sul rilevamento della dinamica di apposizione della firma autografa che può essere utilizzata per la sottoscrizione di documenti informatici, in modo tale che:

1. la firma "autografa" sia strettamente associata al documento oggetto della sottoscrizione (DPCM 22.02.2013, art. 56, c.1, lett. h): "Le soluzioni di FEA garantiscono la connessione univoca della firma al documento sottoscritto");
2. la firma "autografa" protegga l'integrità del documento e della firma stessa come riportata nel documento (DPCM 22.02.2013, art. 56, c.1, lett. d): "Le soluzioni di FEA garantiscono la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma");
3. i dati biometrici di cui è costituita la firma siano adeguatamente protetti in modo che sia impossibile copiarli ed associarli in modo artificiale o fraudolento ad un diverso documento.

Analisi di conformità al provvedimento

In questo paragrafo sono riportate in dettaglio le caratteristiche tecniche della Soluzione di Firma Grafometrica adottate nel presente progetto che sono state implementate in conformità al **Provvedimento generale prescrittivo del Garante per la Protezione dei Dati Personali del 12 novembre 2014**, in particolare nell'art. 4.4, "*Sottoscrizione di documenti informatici*" sottolineando la responsabilità e la competenza di ciascun aspetto."

a) Identificazione del firmatario

lettera a): "Il procedimento di firma è abilitato previa identificazione del firmatario".

L'ottemperanza a questa disposizione compete all'Azienda titolare del trattamento dei dati.
Il processo di sottoscrizione di documenti informatici con FG avviene solo tramite le postazioni di lavoro dedicate e alla presenza di un operatore dell'Azienda che identifica il soggetto che sta per apporre la firma. Tutti i documenti sottoscritti con firma grafometrica da parte di una persona sono subito dopo controfirmati con firma digitale dell'operatore che ha identificato il firmatario. Opzionalmente l'azienda può predisporre una specifica "Procedura operativa di acquisizione di firma grafometrica" ed eventualmente un corso di formazione al quale partecipano tutti gli operatori che raccolgono le firme grafometriche.

b) Sottoscrizione cartacea alternativa

lettera b): "Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici".

L'ottemperanza a questa disposizione compete all'azienda titolare del trattamento dei dati.

L'azienda titolare del trattamento dei dati dovrebbe prevedere sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici, definendoli, preferibilmente, in un'apposita procedura adottata aziendalmente.
È importante sottolineare ai fini archivistici che questi documenti dovranno comunque, indipendentemente dal loro supporto, essere gestiti come parte del patrimonio archivistico dell'azienda, quindi anche per la loro gestione dovranno essere previste delle procedure organizzative condivise in merito a modalità di sottoscrizione, gestione e conservazione.

c) Cancellazione dei dati biometrici grezzi

lettera c): "La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della procedura di sottoscrizione, e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto".

L'ottemperanza a questa disposizione compete al fornitore del sistema di firma grafometrica.
I dati biometrici vengono trasferiti in modo cifrato (con criteri di cifratura messi a disposizione dal produttore dell'hardware stesso) dal dispositivo hardware al software di gestione installato sulla postazione di lavoro dove i dati biometrici vengono elaborati per il tempo brevissimo strettamente necessario per completare la loro cifratura con chiave di cifratura pubblica fornita dalla soluzione di firma. Subito dopo la cifratura, tutti i dati biometrici, che non vengono mai memorizzati su disco, sono cancellati dalla memoria RAM per impedire qualsiasi tipo di trattamento dei dati grezzi.

d) Crittografia dei dati biometrici

lettera d: "I dati biometrici e grafometrici non sono conservati, neppure per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati e certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. La corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di FG può conservare in modo completo tale chiave privata. Le modalità di generazione, consegna e conservazione delle chiavi sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1 lettere e) ed f) del D.P.C.M. 22 febbraio 2013".

L'ottemperanza a questa disposizione compete al fornitore del sistema di firma grafometrica.
Per impedire a chiunque di accedere ai dati biometrici, non appena completata la sottoscrizione grafometrica su appositi dispositivi di acquisizione, i dati biometrici sono memorizzati in documenti informatici in forma cifrata con sistemi di crittografia a chiave pubblica la cui corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario definito dall'azienda erogatrice del servizio in accordo con il fornitore del servizio di firma. Il "soggetto terzo fiduciario" fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. Le modalità con cui l'Azienda sanitaria può richiedere le operazioni di disclosure per estrarre la FG cifrata da uno o più specifici documenti di cui l'azienda stessa risulta titolare ai fini di perizie grafometriche devono essere definiti dall'azienda sanitaria stessa con il fornitore della soluzione di firma. Il soggetto terzo fiduciario potrà procedere alla disclosure su ordine del Giudice o richiesta dell'azienda sanitaria. La richiesta dell'azienda sarà però ammessa soltanto se si abbia il concorso di un perito professionalmente qualificato e

se la richiesta stessa sia funzionale a procedure giudiziarie che vedano l'azienda contrapposta al firmante, suoi aventi causa od altro soggetto portatore di un interesse giuridicamente rilevante. Sono equiparati al giudizio l'arbitrato, la mediazione e ogni altra procedura diretta alla composizione delle controversie che sia conforme alle norme e/o alle best practices professionali pro tempore applicabili.

e) Trasmissione dati biometrici

lettera e): La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati".

L'ottemperanza a questa disposizione compete al fornitore del sistema di firma grafometrica.
I dati biometrici acquisiti dal dispositivo hardware di acquisizione vengono trasferiti al modulo software, che si occupa del loro inserimento all'interno del documento informatico, in modo cifrato utilizzando i criteri di cifratura messi a disposizione dal produttore dell'hardware stesso. La comunicazione tra la postazione di lavoro per l'acquisizione della firma grafometrica e il Server della soluzione avviene con protocollo cifrato https. Tutte le altre comunicazioni gestiscono dati cifrati nelle modalità descritte nel paragrafo che risponde alla lettera d) del provvedimento prescrittivo del Garante Privacy del 12.11.2014 (Crittografia dei dati biometrici).

f) Protezione delle postazioni di lavoro

lettera f): "Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati".

L'ottemperanza a questa disposizione compete all'azienda titolare del trattamento dei dati.
Tutte le postazioni di lavoro FG dell'azienda devono essere utilizzabili solo dagli operatori autorizzati che operano come utenti non amministratori di sistema e che abbiano disabilitato qualsiasi funzionalità di installazione software. L'installazione del software che consente la firma grafometrica e l'installazione degli strumenti che consentono la cifratura dei dati biometrici, devono essere effettuate in modo sicuro secondo una procedura di installazione che l'azienda sanitaria deve richiedere al fornitore della soluzione di firma e inserire nella documentazione formale di ottemperanza al provvedimento prescrittivo del Garante della Privacy.

g) Firewall e protezione da azioni di malware.

lettera g): "I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati".

L'ottemperanza a questa disposizione compete all'azienda titolare del trattamento dei dati.
L'azienda ha adottato specifici sistemi di firewall per la protezione del perimetro della rete previsto e contro i tentativi di accesso non autorizzato ai dati. L'azienda sanitaria dovrà provvedere a fornire un'idonea descrizione delle politiche di sicurezza adottate.

h) Mobile e BYOD (Bring Your Own Device)

lettera h): Nel caso di utilizzo di sistemi di FG nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri

equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).

L'ottemperanza a questa disposizione compete al fornitore del sistema di firma grafometrica.
L'azienda sanitaria deve richiedere al fornitore del servizio di firma una descrizione delle modalità di gestione delle postazioni di firma di tipo mobile o su dispositivi di proprietà di soggetti terzi.

i) Certificazioni digitali e policy di sicurezza

lettera i): "I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi)".

L'ottemperanza a questa disposizione compete al fornitore del sistema di firma grafometrica.
L'Azienda sanitaria deve richiedere al fornitore del servizio di firma una descrizione delle funzionalità di remote wiping nel caso siano previsti dispositivi mobile.
Nel caso, invece, non siano previste postazioni di tipo mobile non sarà prevista alcuna funzionalità di remote wiping, tuttavia sarà necessario fornire una descrizione dello scenario in cui i dispositivi dovessero essere sottratti o smarriti, modalità di impedimento del loro riutilizzo etc.

j) Accesso al modello grafometrico (Esibizione/Disclosure)

lettera j): "L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla FG da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1, lettere e) ed f) del D.P.C.M. 22 febbraio 2013".

L'ottemperanza a questa disposizione compete al fornitore del sistema di firma grafometrica.
L'accesso ai dati grafometrici avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario di cui al paragrafo afferente alla lettera d) del provvedimento prescrittivo del Garante Privacy - Crittografia dei dati biometrici) nei soli casi indicati nello stesso paragrafo.
Sono di pertinenza dell'azienda sanitaria l'individuazione di una procedura di disclosure e l'Informativa resa agli interessati contenente le condizioni e le modalità di accesso alla FG da parte del soggetto terzo fiduciario o da parte di tecnici qualificati. Inoltre, è opportuno che in questa procedura fossero indicati anche gli aspetti tecnologici (strumenti, software, etc.) che consentano lo svolgimento di una perizia grafotecnica da parte di un grafologo.

k) Relazione descrittiva del trattamento

lettera k): "E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante. I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di

redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico".

L'ottemperanza a questa disposizione compete all'azienda titolare del trattamento dei dati.
La relazione richiesta dal Garante della Privacy non è altro che un documento che raccolga la descrizione di tutti i punti sopra esposti, vale a dire una relazione che dia evidenza dell'ottemperanza della soluzione di FG alle prescrizioni previste dal Garante stesso.
Questa relazione viene predisposta dal Responsabile Privacy dell'azienda Titolare del Trattamento e viene conservata dal Titolare del trattamento. Questa relazione viene aggiornata annualmente per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante per la protezione dei dati personali.

Documentazione associata al processo di gestione della firma grafometrica

In questo paragrafo viene descritta la documentazione formale necessaria per la corretta dematerializzazione del processo stesso.

La normativa citata nei precedenti paragrafi, infatti, è molto chiara ed esplicita in merito ai documenti che devono accompagnare le fasi di digitalizzazione dei flussi e che garantiscono la presenza di tutti i prerequisiti necessari. Ogni passo della gestione dei consensi digitali è caratterizzato, dalla produzione e gestione di opportuna documentazione, strettamente riferita ad un particolare articolo o aspetto della normativa.

a) Polizza assicurativa

Le nuove Regole Tecniche in materia di Firme Elettroniche specificano che i soggetti, che adottano un procedimento di firma grafometrica, devono dotarsi di una specifica polizza assicurativa che protegga i titolari da eventuali danni derivanti dalla procedura applicata. Il riferimento normativo relativo alla richiesta di Polizza Assicurativa è costituito dal **DPCM del 22 febbraio 2013, Art. 57 – comma 2**, di seguito riportato *"al fine di proteggere i titolari della FEA e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, i soggetti di cui **all'art. 55, comma 2, lettera a)**, si dotano di una copertura assicurativa per la responsabilità civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ad euro cinquecentomila"*.

b) Adesione e Revoca al Servizio FEA

Sempre all'interno delle Regole Tecniche in materia di Firme Elettroniche si specifica l'importanza che l'applicazione della FG su un documento informatico da parte di un paziente o di un utente venga effettuata in modo consapevole. Per questo motivo, all'interno dell'Azienda che eroga servizi di FEA deve essere prevista la sottoscrizione preventiva, da parte del firmatario, di uno specifico consenso all'uso della FEA e al trattamento dei dati biometrici. Tale consenso, in più, deve essere in ogni momento revocabile da parte del firmatario stesso. I riferimenti normativi relativi all'obbligo di raccolta di uno specifico consenso, nella forma di dichiarazione di accettazione delle condizioni del servizio, da parte del titolare di firma, all'uso della FEA Grafometrica e della possibilità di revoca dello stesso consenso in qualsiasi momento, sono esplicitati all'art. 57 del DPCM del 22 febbraio 2013.

c) Informativa sulla FEA

La normativa sulla FEA nonché il Provvedimento del Garante della Privacy e il Codice della Privacy (D.lgs. 196/2003) insistono sull'obbligo di rendere disponibili a tutti i possibili fruitori del servizio di FEA informazioni chiare e esaustive su come essa venga gestita all'interno della Struttura in esame, nonché sui diritti degli interessati. Tali informazioni devono essere facilmente accessibili da parte degli utenti e devono permettere loro di assumere piena consapevolezza sulla modalità di firma che stanno adottando. Il mezzo per garantire la massima accessibilità a queste informazioni è la loro pubblicazione sul sito web aziendale. I riferimenti normativi relativi all'obbligo di informazione chiara e esaustiva all'interessato sulle modalità di applicazione della firma grafometrica all'interno della propria Struttura, inclusi i dettagli su come aderirvi o su come revocarne il consenso, sono esplicitati all'art. 57 del DPCM del 22 febbraio 2013, all'art. 7 e 13 del Codice Privacy e nel Provvedimento prescrittivo n.513 del Garante della Privacy del 12 novembre 2014.

d) Descrizione del sistema e delle tecnologie che sottendono alla gestione della FEA

Sempre in riferimento all'Informativa che le Norme indicano di mettere a disposizione dell'utente finale, è espressamente richiesto che essa sia accompagnata da informazioni tecniche dettagliate sulla soluzione software e hardware adottata per la gestione della FEA. La normativa prevede in modo esplicito che la descrizione delle caratteristiche del sistema e delle tecnologie utilizzate siano pubblicate sul sito web della Struttura erogante (**DPCM 22.02.2013, art. 57, comma 1, lettere e), f)**). L'Azienda erogante la soluzione di firma grafometrica ha quindi il compito di pubblicare, sul proprio sito, una descrizione tecnica accurata sul prodotto e sull'infrastruttura scelti per l'applicazione della FG sui documenti, in particolare sui consensi informati digitali, dimostrando nel contempo il rispetto dei prerequisiti richiesti. I riferimenti normativi relativi all'obbligo di informazione chiara e esaustiva al paziente sulle modalità di applicazione della firma grafometrica all'interno della propria Struttura.

e) Notificazione al Garante della Privacy

La gestione della FEA grafometrica comporta necessariamente l'acquisizione, oltre che del glifo, anche dei parametri biometrici del titolare di firma quali la pressione e la velocità della firma. La gestione di tali parametri, al pari del trattamento dei dati sensibili, comporta per la Società erogante l'obbligo di notificazione al Garante secondo la procedura messa a disposizione sul suo stesso sito, come previsto dal codice della Privacy (**D. lgs 196/2003, art. 37 comma 1, lettera a**). La notificazione è una dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali, svolta quale autonomo titolare del trattamento.

f) Istanza di verifica preliminare al garante per la Privacy

Il Garante della Privacy, prevede che prima di avviare il trattamento di dati biometrici si debba presentare al Garante stesso un'istanza di verifica preliminare (**Provvedimento prescrittivo Garante 12.11.2014 , Allegato A).**

Il provvedimento prescrittivo del 12 novembre 2014 stabilisce che, nell'ambito della sottoscrizione di documenti informatici (paragrafo nr. 4.4) , il soggetto erogatore può essere esonerato dalla presentazione di questa istanza di verifica preliminare predisponendo una dichiarazione di conformità al Provvedimento stesso. Tale dichiarazione deve contenere la descrizione di come il trattamento dei dati sia svolto nel rispetto di specifiche prescrizioni e limitazioni, che sono in parte di carattere tecnico, in parte di carattere organizzativo.

g) Procedure interne

A latere della documentazione formale richiesta dalla normativa, è consigliabile che la Struttura erogante adotti specifiche procedure organizzative che chiariscano alcuni aspetti specifici legati alla gestione dei processi di:

a) Adesione al servizio di FEA;
b) Sottoscrizione di documenti informatici con firma grafometrica;
c) Gestione del Data breach (violazione dei dati);
d) Esibizione di documenti informatici sottoscritti con firma grafometrica.

Queste procedure devono essere definite e approvate dalla struttura erogante e condivise con tutti i soggetti coinvolti.

E' anche fondamentale che il paziente possa facilmente accedere alle informazioni relative a:

- come poter revocare il consenso;
- come poter avere una copia dei consensi sottoscritti e della eventuale revoca.

Tali informazioni devono essere rese disponibili direttamente nell'informativa pubblicata sul sito aziendale.