

MISURE MINIME			MISURA GIA IN ESSERE	MISURA DA ADOTT.	STRUTTURA O PERSONE ADDETTE ALL'ADOZIONE
1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.	Credenziali e procedura di autenticazione				
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.	Codice di identificazione personale e parola chiave riservata				
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.	Credenziali individuali	Attivazione o Implementazione della Policy di Sistema			
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.	Istruzioni di diligente custodia	Istruzioni per gli amministratori di sistema			
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.	Lunghezza della password pari a 8 caratteri o pari al massimo consentito dal sistema	Adeguamento per consentire l'adozione di password con lunghezza di almeno 8 caratteri			
	Controllo sulla complessità della password	Istruzioni per gli incaricati			
	Modifica password al primo accesso	Attivazione della policy se disponibile sul sistema			
	Possibilità di sostituzione autonoma della password	Istruzioni per gli incaricati			
	Scadenza della password per dati sensibili e giudiziari entro 3 mesi	Attivazioni delle Policy su tutte le piattaforme			
		Attivazione della policy se disponibile sul sistema			
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.	Il codice identificativo deve essere univoco	Istruzioni per gli amministratori di sistema			
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.	Scadenza delle credenziali non utilizzate da 6 mesi	Attivazione della policy se disponibile sul sistema			

MISURE MINIME			MISURA GIA IN ESSERE	MISURA DA ADOTT.	STRUTTURA O PERSONE ADDETTE ALL'ADOZIONE
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.	Disattivazione delle credenziali in caso di perdita della qualità per l'accesso	Policy per Uff. del Personale, Responsabili Amm. Di sistema			
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.	Istruzioni per l'incaricato a non lasciare incustodito lo strumento elettronico in caso di prolungata assenza dal posto di lavoro	Automatismi di logoff a tempo quando disponibili ovvero adozione di SceenSaver e configurazione dei medesimi			
		Istruzioni per gli incaricati Istruzioni per gli amministratori di sistema			
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.	Gestione delle credenziali in caso di prolungata assenza o impedimento dell'incaricato per la disponibilità dei dati o degli strumenti elettronici	Procedura per la conservazione cartacea delle password in presenza di trattamenti particolari effettuati da incaricati su sistemi stand alone			
		Istruzioni per gli incaricati			
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.					
12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.	Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione	Implementazione di un sistema di profilatura delle autorizzazioni			
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.	Assegnazione dei profili per utente o classi omogenee di utenti anteriormente all'inizio del trattamento	Policy di Sicurezza e processo di nomina degli Incaricati a cura Uff. del Personale, Responsabili			
		Istruzioni per gli amministratori di sistema			
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	Verifica della sussistenza delle condizioni per la conservazione dei profili (almeno annualmente)	Procedura di verifica a cura dell'Uff. del Personale, Responsabili, Amm. Di Sistema			

MISURE MINIME		MISURA GIÀ IN ESSERE	MISURA DA ADOTT.	STRUTTURA O PERSONE ADDETTE ALL'ADOZIONE
15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.	Individuazione con cadenza almeno annuale della lista degli incaricati anche organizzata per classi omogenee di incarico e relativi profili di autorizzazione	Procedura di verifica a cura dell'Uff. del Personale, Responsabili, Amm. di Sistema e tenuta dell'elenco		
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.	Protezione dei dati dal rischio di intrusione e dall'azione di programmi pericolosi (aggiornamento almeno semestrale)	Presenza di un processo formalizzato di gestione e verifica del sistema Anti-Virus su Server e pdl		
		Processo formalizzato di gestione e verifica del sistema Anti-Virus su Server e pdl		
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.	Programmi per elaboratore atti a prevenire vulnerabilità degli strumenti elettronici aggiornati almeno annualmente, o semestralmente per i dati sensibili o giudiziari	Processo formalizzato di verifica e gestione della configurazione dei sistemi (hardening) e degli apparati di rete e produzione di verbali		
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.	Istruzioni organizzative e tecniche che prevedono il salvataggio dei dati almeno settimanalmente	Istruzioni per gli amministratori di sistema		
20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.	Protezione dei dati sensibili e giudiziari contro l'accesso abusivo di cui all'art. 615-ter, mediante utilizzo di strumenti elettronici	Presenza di un processo formalizzato di gestione e		
		Processo formalizzato di gestione e verifica dei sistemi firewalls, ecc		
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.	Controllo sull'utilizzo dei supporti rimovibili di memorizzazione ad evitare l'accesso non autorizzato o il trattamento non consentito	Processo di controllo formalizzato per l'uso dei supporti di memorizzazione		
		Istruzioni per gli amministratori di sistema Istruzioni per gli incaricati		
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.	Distruzione dei supporti rimovibili non più utilizzati contenenti dati sensibili / giudiziari o riutilizzo solo se le informazioni precedentemente contenute non possono essere tecnicamente ricostruibili	Processo formalizzato per la distruzione dei supporti di memorizzazione		
		Istruzioni per gli amministratori di sistema		

MISURE MINIME		MISURA GIÀ IN ESSERE	MISURA DA ADOTT.	STRUTTURA O PERSONE ADDETTE ALL'ADOZIONE
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.	Misure di ripristino per l'accesso ai dati in caso di danneggiamento degli stessi e degli strumenti in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni	Delineazione delle esigenze del cliente sulla base della tipologia dei dati e delle verifiche sulle soluzioni già adottate		
		Procedure operative formalizzate e documentazione aggiornata		
		Istruzioni per gli amministratori di sistema		
		Approvvigionamento e gestione dei media		
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.	Cifratura, codici identificativi o separazione dei dati su sistemi distinti per il trattamento dei dati sensibili e giudiziari atti a prevenire l'accesso a persone prive di autorizzazione.	Implementazione di un sistema di cifratura (hw/sw) ed eventuali adeguamenti post verifica		
		Procedure operative formalizzate e documentazione aggiornata		
	Locali attrezzati di opportune misure di sicurezza per il trattamento di dati idonei a rivelare l'identità genetica degli interessati.			
	Il trasporto all'esterno dei dati genetici deve avvenire solo con contenitori muniti di serratura.			
	Il trasferimento dei dati in formato elettronico dei dati genetici è cifrato.			
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.				
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.	Attestazione di Avvenuta redazione del DPS e citazione nella relazione accompagnatoria del bilancio.			

MISURE MINIME		MISURA GIÀ IN ESSERE	MISURA DA ADOTT.	STRUTTURA O PERSONE ADDETE ALL'ADOZIONE
27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.	Istruzioni per l'incaricato atte al controllo e custodia degli atti e documenti. Mantenimento di un aggiornato elenco degli incaricati e del loro profilo di autorizzazione con cadenza annuale	Procedure operative formalizzate e documentazione aggiornata		
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.	Istruzioni per la custodia e il controllo di atti e documenti contenenti dati sensibili o giudiziari	Procedure operative formalizzate e documentazione aggiornata		
29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.	Controllo di accesso agli archivi contenenti dati sensibili o giudiziari	Istruzioni per gli incaricati		
	Le persone autorizzate all'accesso fuori dall'orario di ufficio sono individuate e registrate.	Procedura organizzativa (vigilanza e addetti alle pulizie, o dipendenti) formalizzate e documentazione aggiornata		
	In mancanza di strumenti elettronici per il controllo degli accessi nei locali o di personale di vigilanza, le persone abilitate all'accesso sono preventivamente autorizzate.	Procedura formalizzata di autorizzazione per l'accesso ai locali		