Handbok för IT användare på SÄS

2017-01-01

Stefan Fransson
Informationssäkerhetssamordnare
Personuppgiftsombud SÄS
FC plan2, 501 82 Borås
Tfn: 033 616 1329, 070 566 9302
e-post: stefan.fransson@vgregion.se

Informationssäkerhet

Mål

Målet med denna handbok är att ge en hjälp till användare av de IT-system som finns på SÄS. Handboken kan användas av alla verksamhetsområden på SÄS för att få reda på vilka krav som finns när det gäller informationssäkerhet.

För mer information och kunskap angående informationssäkerhet besök hemsidan SIW/Tjanster-och-verktyg/IT-telefoni/IT-informationssakerhet

Vad är informationssäkerhet?

Mycket av vår information är mycket värdefull för oss, ibland till och med livsviktig. Tänk till exempel på informationen i patientjournaler. Är informationen förlorad eller felaktig kan det få katastrofala följder.

Därför måste vi skydda vår information så:

- att den alltid finns när vi behöver den (*tillgänglighet*)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (*riktighet*)
- att endast behöriga personer får ta del av den (*konfidentialitet*)
- att det går att följa hur och när informationen har hanterats och kommunicerats (*spårbarhet*)

Skyddet behöver givetvis anpassas efter behovet så att det inte är för klent eller alltför krångligt och dyrt. Men med tanke på vad konsekvenserna kan bli med bristande skydd kan detta inte försummas av vare sig enskilda eller organisationer. God informationssäkerhet skall vara en självklarhet för alla.

Skydda dina tillgångar

Informationssäkerhet omfattar både administrativa rutiner med policys och riktlinjer och tekniskt skydd med bland annat brandväggar och kryptering. Det handlar om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge organisationens information det skydd den förtjänar.
Metoder som används när det gäller informationssäkerhet är riktlinjer och regelverk och man inriktar sig mot begreppen *Tillgänglighet*, *Sekretess*, *Spårbarhet* och *Oavvislighet*

Information och data är en av många viktiga resurser för SÄS. Numera finns all vår patient och personalinformation i olika IT-system och de olika verksamheterna inom SÄS förvaltar stora mängder information som rör både patienter och anställda. Fel hantering av känslig information kan orsaka stor skada för den som drabbas.
Syftet med allt säkerhetsarbete är att skapa en trygghet för verksamheten och dess verksamhet men även en trygghet för att patienters och anställdas uppgifter hanteras på ett korrekt och säkert sätt.

Andras ansvar

Sjukhusledningen har alltid det övergripande ansvaret för verksamheten och de IT-system som används som stöd i denna. Eftersom informationssäkerheten ingår som en naturlig del i ett IT-system ligger därmed också det generella ansvaret för informationssäkerhet hos sjukhusledningen.

Delegering av ansvaret för Informationssäkerheten sker normalt enligt samma principer som gäller för delegering av verksamhetsansvaret inom organisationen. Under ledningen är alltså var och en, som är ansvarig för någon del av verksamheten, också ansvarig för informationssäkerheten inom sitt område. Detta generella ansvar sträcker sig ner till den enskilde användaren.

Utförarstyrelsen är personregisteransvarig enligt Personuppgiftslagen. På SÄS finns ett Personuppgiftsombud vars uppgift är att se till att de personregister som finns behandlas på ett korrekt sätt i förhållande till lagen. Alla personregister som finns på SÄS skall finnas med i den personregisterförteckning som förs på SÄS och det är därför tvång på att alla personregister som skapas måste anmälas till personuppgiftsombudet på SÄS. Personuppgiftsombud på SÄS är Stefan Fransson, kanslienheten. Läs mer om behandling av personuppgifter på SIW sida: SIW/Tjanster-och-verktyg/IT-telefoni/Behandling-av-personuppgifter

Eget ansvar

Som användare av ett IT-system är Du skyldig att känna till och följa de föreskrifter om informationssäkerhet som gäller på SÄS och på Din arbetsplats.

När Du börjar arbeta med datorutrustning och programvara, måste Du se till att Du får sådan information och utbildning att Du kan utföra Dina arbetsuppgifter på ett riktigt sätt. Du ska också känna till på vilket sätt konstaterade brister ska rapporteras.

Behörighet och lösenord

Behörighet att använda IT-systemen på SÄS är en rättighet som du som anställd erhåller. Att ha en viss behörighet innebär inte bara rättigheter att få utföra vissa arbetsuppgifter utan också skyldigheter.
För att säkra behörigheten när du arbetar i olika IT-system har du ett användar-ID och ett lösenord.
På SÄS finns det flera behörighetskontrollsystem som reglerar åtkomsten till olika delar av IT-systemen, och som även reglera vem som får göra vad i ett system.
Ett behörighetskontrollsystem är till för att de som finns registrerade i olika personregister skall kunna känna sig trygga och veta att ingen obehörig kan komma åt den information som finns.
Behörighetskontrollsystemet skall dessutom skydda den egna personalen. Ingen skall behöva bli oskyldigt misstänkt eller beskylld för fel, misstag eller annat som någon annan gjort. Därför finns i de flesta IT-system händelseloggar som visar vilken användare det är som har varit och jobbat i systemet och vad den personen har gjort. Om en obehörig transaktion spåras till ditt användar-ID - och du har lånat ut det till en arbetskamrat - kan du hamna i en besvärlig situation.

Inom SÄS strävar vi efter att varje medarbetare skall ha ett eget unikt användar-ID. Det finns arbetsplatser inom SÄS där detta av praktiska skäl inte låter sig göras, utan man tvingas då vara flera medarbetare som delar på ett användar-ID, ett s.k. gemensamt användar-ID. Beslut om att använda ett gemensamt användar-ID kan endast fattas av IT-säkerhetssamordnaren eller VGR-IT, inte lokalt på enheterna.

Lösenord skall vara uppbyggda så att de inte går att gissa sig till. Samtidigt får de inte vara så komplicerade och svåra att man inte kommer ihåg dem. Ha inte fler eller svårare lösenord än att du kommer ihåg dem. Om du behöver skriva ner dina lösenord på en lapp för att komma ihåg dem så är de felkonstruerade

Användar-ID och lösenord får aldrig vara identiska med varandra. Använd inte lättgissade lösenord, t ex för- eller efternamn, företagsnamn, bilmärken, personnummer eller liknande.

Lösenord skall bytas när du blir ombedd av systemet att göra så, eller var 90: e dag. Även där man har gemensamt användarkonto skall det finnas rutiner för att byta lösenord.
Har du glömt ditt lösenord tar du kontakt med VGR-IT som hjälper dig att lösa problemet

Händelseloggar

Arbetsgivarens rätt till kontroll.
En grund för att kunna ha en god informationssäkerhet är att det finns händelseloggar i de olika IT-systemen. En händelselogg visar vilken användare det är som har jobbat i systemet, och alla de händelser som den användaren utfört. På SÄS finns dessa loggar i ett flertal system, bland annat i våra journalsystem, i de personaladministrativa systemen och för Internet. För de olika systemen finns det personer utsedda som sköter om kontrollen av loggarna.
Det finns ett centralt loggsystem installerat på SÄS. Detta system används av VGR-IT för att inventera den hårdvara och de program som finns installerat i nätverket. Anledningen är i första hand felsökning/hantering och kapacitetsuppföljning men system kommer även att användas för att söka efter piratkopierade program och andra otillåtna installationer i vårt nätverk.

All användning av Internet registreras i en logg. Loggen omfattar uppgifter om användarnamn och namnet på den webbplats som besöktes. Vid misstanke om missbruk av Internet kommer loggen att användas för kontroll av vad som är gjort och vem som har gjort det.

Det förs en logg över all e-post som innefattar uppgifter om avsändare, mottagare, ärendemening, tidpunkt, storlek samt bifogade kopior. Arbetsgivaren (SÄS) utövar ingen kontroll över de anställdas e-postmeddelande. Arbetsgivaren kan komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet. Arbetsgivaren kan även komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt vid fara för informationssäkerhet, t.ex vid virus- och hackerangrepp, eller för att utreda och förhindra brott.

Överträdelse av reglerna
Om det av kontrollerna framgår att riktlinjerna överträtts eller att svensk lag har brutits kommer ärendet att utredas av verksamhetschefen och representanter från SÄS personalenheten.
Den som bryter mot uppsatta regler kan bli föremål för disciplinära åtgärder.

Felrapportering.

Du skall alltid rapportera de avvikelser och felaktigheter du upptäcker i datorns och programmets funktioner. Detta behövs som underlag för att analysera och avhjälpa de fel som finns och för att vidta säkerhetshöjande åtgärder.
Du skall använda samma system för att rapportera denna typ av avvikelser/fel som du använder när du rapporterar andra avvikelser gällande ex. patient och personal.
För felrapportering av IT-incidenter skall MedControl PRO användas

Allmän Informationssäkerhet

Utskrifter.
Skrivare skall stå där endast behöriga kan ta del av utskrifterna. Utskrifter av dokument på gemensamma skrivare skall hämtas så snart du kan. Tänk på att kvarglömda dokument kan komma i orätta händer.
Detsamma gäller för fax och kopieringsmaskiner, kvarglömda dokument kan komma i orätta händer. I nyare faxar och kopieringsmaskiner finns det stora minnen där de faxade/kopierade sidorna sparas. Tänk på detta då det skall göras service på denna typ av utrustning. Ett knapptryck av servicemannen och de senast faxade/ kopierade sidorna skrivs ut igen.
Vid vissa tillfällen är det nödvändigt att man skickar fax innehållande känslig information, ex. patientuppgifter. Vid dessa tillfällen skall man använda rutinen ”Säker fax” som beskrivs senare i denna skrift.

Bildskärmen.
Se till så att datorer inte står placerade så att obehöriga lätt kan läsa från dess bildskärm, ex. i receptioner och kassor. Det finns filter att använda som förhindrar obehöriga att läsa på skärmen.
När du lämnar din arbetsplats obevakad kan den användas av obehöriga. Ibland kan du bli borta längre än tänkt från arbetsplatsen. Gör därför till vana att alltid aktivera en skärmsläckare med lösenord när du lämnar din arbetsplats.

Säkerhetskopiering
Säkerhetskopiering av information som finns lagrad på server ansvarar VGR-IT för. Det tas kontinuerligt säkerhetskopior på all information som sparas på de olika servrarna i vårt nätverk. Information som du sparar lokalt på din egen pc:s hårddisk, ofta C:, ansvarar du själv för när det gäller säkerhetskopiering. Speciellt viktigt för dig som har bärbar dator och då kanske sparar på lokal hårddisk.

Program
Endast program licensierade för arbetsgivaren får installeras och/eller användas på datorer inom SÄS. All kopiering till SÄS datorer av programvaror som någon annan har upphovsrätten till är förbjuden. Innan man skaffar en programvara för installation på dator inom SÄS skall VGR-IT kontaktas. Detta för att kontrollera att det är en programvara som fungerar i vår IT-miljö och inte stör andra, redan installerade IT-system.

Virus.
Alla persondatorer på SÄS skall vara försedda med ett fungerande antivirusprogram. SÄS har antivirusprogram installerat i servrar och lokalt på varje pc. Trots detta skall man alltid tänka sig för innan man öppnar e-post från okända avsändare. Vem är det ifrån? Varför skickas det till mig? ”Tänk efter före” innan du dubbelklickar på ett bifogat dokument
En annan typ av "virus" är e-kedjebrev, exempelvis när man skickar ut en falsk virusvarning och ber mottagaren skicka det vidare till alla han känner. Dessa e-kedjebrev skadar inte någon pc eller annan hårdvara men om alltför många inom SÄS börjar skicka runt dessa e-kedjebrev kan mängden information som skickas i nätverket bli så stor att nätverket stannar eller går mycket långsamt**.**

Inom SÄS är det endast VGR-IT eller IT-säkerhetssamordnaren som går ut med virusvarningar.

Skrotad datautrustning
Datautrustning och olika typer av datamedia som har tjänat ut måste förstöras. En CD skiva är relativt enkel att förstöra medan andra saker, ex. datorer, skrivare, bildskärmar, databand mm kan vara svårare att förstöra.
När datorutrustning inte längre ska användas på SÄS skall den tas omhand på ett säkert och miljömässigt riktigt sätt. Detta innebär att ingen utrustning får lämna SÄS utan att eventuell känslig information är säkert raderad, eller på annat sätt garanterad att den inte kan ses av obehöriga.
All den utrustning som ingår i PC utbytet och som byts av VGR-IT regelbundet var tredje år raderas på ett säkert och kontrollerat sätt.
Läs mer i riktlinje: Skrotning eller avyttring av elektronisk utrustning dnr:10971

Elektronisk post
På SÄS är vi stora användare av e-post. Detta innebär att e-postanvändandet är en vital funktion för SÄS som varje användare måste hantera varsamt. Detta gör det nödvändigt att ha gemensamma regler att följa. Offentlighetsprincipen, Personuppgiftslagen, Förvaltningslagen och Arkivlagen är de lagar som i första hand berör E-post. Dessa lagar är teknikneutrala och det är därför ingen skillnad på E-post och konventionellt befordrad post.

För information om loggning av användandet av e-post läs avsnitt ”Händelseloggar” i början på denna riktlinje.

Följande gäller för SÄS och användandet av e-post:

- För att få skicka känslig information med E-post måste informationen krypteras.
- Det är förbjudet att skicka privat e-post från din SÄS e-brevlåda.

Mottagen privat post skall omedelbart gallras. Får du ett e-brev från en patient skall du hantera det som om det vore ett vanligt brev som kom med posten, det skall antecknas och journal- eller diarieföras. Meddela sedan patienten att du inte kan kommunicera via e-post utan hänvisa till ”Mina Vårdkontakter”.

Använd funktionen delegera när andra ska sköta din e-brevlåda, ex. vid längre frånvaro. Din E-postlåda får lika lite som din brevkorg ligga oläst vid frånvaro. När du använder din e-post i tjänsten så representerar du SÄS. Tänk på vad du skriver och vem du skickar till.

Funktionsbrevlåda
En funktionsbrevlåda måste alltid bevakas, även vid semesterstängning, av enheten. Detta följer av de regler som finns i framför allt tryckfrihetsförordningen, sekretesslagen och arkivlagen om att allmänna handlingar skall registreras, bevaras och hållas tillgängliga för press och allmänhet. Någon vid en annan enhet kan ges uppdrag och behörighet att öppna brevlådan och läsa e-posten.
Det är ett krav för att ha en funktionsbrevlåda, att posten tas om hand även under semestern. Ett automatiskt svarsmeddelande kan inte ersätta detta.
Det finns ingen funktion för att aktivera "Ej på kontoret" på funktionsbrevlådor. Vidaresändning fungerar inte heller på dessa brevlådor.

Konsulter
All icke anställd personal som i en eller annan funktion kan komma i kontakt med IT-resurser eller IT-funktioner skall skriva på ett tystnadspliktsavtal. Det gäller konsulter,

leverantörer, servicepersonal m.fl. Samtidigt som konsulten skriver på avtalet skall han/hon få information om de regler som gäller för IT-hanteringen inom SÄS.

Personberoende
Alla datoriserade arbetsuppgifter på en arbetsplats skall kunna utföras av minst två personer inom samma arbetsplats. Detta för att minimera risken för att det plötsligt inte finns någon som vet hur programmet fungerar.

Bärbara datorer
Bärbara datorer är stöldbegärliga. Förutom den rent ekonomiska förlust som drabbar SÄS finns det stor risk för att känslig information kan komma att läsas av obehöriga. På en bärbar dator sparar man ofta information på datorns egen hårddisk och inte på en server som finns placerad i nätverk. Detta innebär att du som användare själv ansvarar för att det körs säkerhetskopior på all information som finns sparad på den bärbara datorn. Det krävs inte heller något lösenord för att starta en bärbar dator och läsa all information som finns i den.

Den som skapar och sparar information på en bärbar dator är ansvarig för att informationen skyddas på ett sådant sätt att den inte kan läsas av obehöriga.

Alla de bärbara datorer som används på SÄS skall skyddas utifrån vilken information som finns på dem och hur datorerna skall användas. Lagras känslig information på dem skall det finnas ett skydd mot obehörig användning installerat på dem. Som exempel på känslig information kan nämnas identifierbara patientuppgifter, personaluppgifter och vissa typer av ekonomisk information.
Kontakta IT-säkerhetssamordnaren eller VGR-IT för en diskussion angående skydd på era bärbara datorer.

USB Minnen
Ett USB minne är ett litet, flyttbart minneskort som rymmer stora mängder information. Det unika med USB minne är att det läser och skriver mycket snabbt samtidigt som det är väldigt kompakt och pålitligt och rymmer väldigt mycket data och information.
Just de egenskaper att ett USB minne kan rymma väldigt mycket information samtidigt som det är så lätt och smidigt att ta med sig kan innebära en fara om man tappar eller glömmer det någonstans. Att bli av med ett USB minne fyllt med patient eller personalinformation kan vara förödande om någon obehörig skulle hitta det.

Den som skapar och sparar information på ett USB minne är ansvarig för att informationen skyddas på ett sådant sätt att den inte kan läsas av obehöriga.

De USB minnen som används på SÄS och där man kan komma att lagra känslig information skall köpas via VGR-IT som då kan levererar ett USB-minne med möjlighet att kryptera informationen och därmed få ett fullgott skydd mot obehörig åtkomst av informationen.

Åtkomstskydd för utrustning och information
Persondatorer med kringutrustning är stöldbegärliga. Den information som finns lagrad i datorn representerar kanske ett ändå större värde, ekonomiskt och arbetsmässigt sett. Vidare kan informationen vara känslig ur sekretessynpunkt.
Det åtkomstskydd man ska välja beror på lokala förutsättningar och skall alltid anpassas till den skyddsnivå som informationsklassificeringen anger.
För datorutrustning som står placerad där det inte går att låsa och/eller larma lokalen ska man överväga att låsa fast utrustningen med speciella vajerlås eller datorboxar.

Låsanordningarna finns att beställa från VGR-IT. Datamedia, CD och liknande, skall förvaras brand- och stöldskyddat.
Informationen skyddas genom att den spara på servrar i nätverket och att det krävs login namn och lösenord för att komma åt den. Finns inte skyddet i form av login namn och lösenord, ex. om man sparar på lokal hårddisk, skall annat skydd av informationen installeras.

Dokumentation
Om du skriver egna program, ex. i Ms Access, som skall användas i verksamheter inom SÄS är det viktigt att du dokumentera program, register och användningen av programmet noggrant. Du kommer troligen inte alltid att vara tillgänglig när problem uppstår, och skulle du lämna din anställning måste det finnas dokumentation över hur programmet fungerar. Köper du ett program av ett företag eller av en kollega måste du se till att erforderlig dokumentation följer med programmet.

Spara dokument
Som standard är persondatorer som används på SÄS inställda så att de med automatik sparar dokument på de klinikgemensamma katalogerna. Vill man spara på egen hemmakatalog betyder det att man manuellt måste styra om val av katalog man vill spara i. När man sparar dokument i den egna hemmakatalogen finns det ingen annan som har tillgång till dessa dokument och skulle man vara frånvarande när någon har behov av just de dokumenten går de ej att få fram.
Har man behov av att begränsa de användare som skall kunna läsa dokumenten finns möjligheten att skapa arbetsgrupper och bara tillåta vissa bestämda användare att komma åt dokumenten. Detta är en funktion som VGR-IT kan stå till tjänst med.

Nätverk och Internet
Användare av SÄS datanätverk och datorer har ett personligt ansvar att följa de regler som gäller för detta. Alla användare är ansvariga för vad som lagras, transporteras och utförs under den/de användaridentitet(er) personen har.

För information om loggning av användandet i Internet läs avsnitt ”Händelseloggar” i början på denna riktlinje.

Varje anställd inom SÄS som brukar Internet via SÄS nätverk är att betrakta som en representant för SÄS. Detta innebär att man har en skyldighet och ett ansvar gällande sitt uppträdande på Internet.

För den information som lagras i SÄS datorer samt transporteras via SÄS nätverk gäller att:

- Informationen inte strider mot svensk lagstiftning.
- Informationen följer god etik.
- Informationen inte kränker andras integritet eller skadar SÄS goda namn och rykte.
- Informationen har anknytning till SÄS verksamhet och dina arbetsuppgifter.

För anställda inom SÄS som på arbetstid använder Internet gäller att:

1. Användning av Internet och dess tjänster ska vara relaterat till dina arbetsuppgifter inom SÄS.
2. Det är endast tillåtet att besöka hemsidor eller länkar vars innehåll överensstämmer med gällande svensk lag. Detta utesluter till exempel sidor som innehåller barnpornografi.

3. Det är endast tillåtet att besöka hemsidor eller länkar vars innehåll är förenligt med en god etik. Det är därför inte tillåtet att besöka webbplatser med extrempolitiskt, pornografiskt eller rasistiskt innehåll, inte heller webbplatser som erbjuder olika typer av spel, ex. poker, tips eller hästar. Det är inte tillåtet att delta i chatt-sidor eller bloggar om de inte är arbetsrelaterade.
4. Det är inte tillåtet att ladda hem program, spel eller annan information från Internet, såvida det inte ska användas i ditt direkta arbete. Se tidigare anvisning i detta dokument kring nyinstallation av programvara.

Det är tillåtet att i begränsad omfattning använda SÄS-datorer för privat Internet-användning. Sådan användning kan innefatta läsande av nyhetssidor, bokning av biljetter/resor, Internetbank. Dock får sådan privat användning aldrig ställas före verksamhetens behov. Nedladdning av filer eller installation av program och programkomponenter får inte förekomma. Dessutom gäller punkterna 2-4 ovan samt att kommunikationen inte direkt eller indirekt får skada SÄS goda namn och rykte. SÄS frånsäger sig allt ansvar för eventuell skada, ekonomisk eller annan, som kan åsamkas den anställde vid privat användning av Internet från SÄS datorer. Arbetsgivaren kan utan föranmälan registrera privat Internetanvändning, på samma sätt som den ordinarie datoranvändningen på SÄS loggas.

Informationsklassning

Varje person som skapar information är också ansvarig för att den blir klassificerad och hanteras på rätt sätt.
Varje chef är ansvarig inom sitt verksamhetsområde för att hemlig och kvalificerat hemlig information skyddas, från det att informationen skapas tills den förstörs.
Varje medarbetare är ansvarig för att inte lämna ut hemlig eller kvalificerat hemlig information till obehörig.

Informationsklassning handlar om att bedöma informationens värde och känslighet. Många brister i nuvarande IT-system beror på att den information som behandlas inte har klassificerats. Man har inte fastställt vilken säkerhetsnivå som är nödvändig för att olika intressenters krav ska kunna tillgodoses.
Informationsägaren har ansvar för informationen från det att den skapas till det att den förstörs. Det betyder att informationsägaren ansvarar för klassning som leder till att informationen skyddas korrekt under hela dess livslängd.
Som hjälp vid klassning av information använder man någon form av riskanalyssystem. Det finns både manuella och datoriserade sådana.
Informationen bedöms utifrån krav inom följande fyra områden:

- **Riktighet**, d.v.s. informationen skall vara korrekt, aktuell och begriplig.
- **Tillgänglighet**, d.v.s. informationen skall vara tillgänglig för behörig användare i beslutad omfattning och på definierad tid.
- **Sekretess**, d.v.s. information och program skall vara skyddad så att de inte avsiktligt eller oavsiktligt görs tillgängliga för obehöriga.
- **Spårbarhet**, d.v.s. funktioner som gör det möjligt att härleda utförda operationer till enskilda användare.

Inom SÄS delar vi upp informationens känslighet i tre klasser:

- **Integritetsklass 3 (grundnivå).** Hit hör den information som betraktas som offentlig och som skall vara tillgänglig för alla, även utanför verksamheten.
- **Integritetsklass 2 (hög nivå).** Hit hör information som betraktas som känslig. Exempel kan vara patientjournaler, olika typer av personaluppgifter,

ekonomiska uppgifter. Denna klass kräver en högre nivå på det skydd som skall finnas för informationen

- **Integritetsklass 1 (mycket hög nivå).** Hit hör den information som har den högsta känsligheten. Exempel kan vara uppgift om tvångsingripande, uppgifter om HIV och AIDS, genforskning och liknande. Kraven på de skyddsåtgärder som skall finna för att skydda informationen är höga. Ofta krävs förhandsgranskning från Datainspektionen för denna typ av register.

Behandling av Personuppgifter

Varje åtgärd, eller serie av åtgärder, som vidtas i fråga om personuppgifter är en ”behandling av personuppgifter”, eller det många i dagligt tal kallar ett personregister. Enligt lagens definition är en personuppgift all slags information som direkt eller indirekt kan hänföras till en person som är i livet.
Det är Styrelsen för SÄS som är personuppgiftsansvarig för de behandlingar av personuppgifter som sker inom sjukhuset.
Styrelsen för SÄS har utsett ett personuppgiftsombud som har till uppgift att se till att behandlingen av personuppgifter sker på ett lagligt och korrekt sätt.
Personuppgiftsombudet har skyldighet att föra en förteckning över samtliga de personregister som finns på SÄS.
Handläggning vid anmälan om behandling av personuppgifter:

Om ny anmälan fordras skall en skriftlig ansökan fyllas i.
Anmälan skickas till sjukhusets personuppgiftsombud. Ansökningsblanketten finns på sjukhusets hemsida för behandling av personuppgifter.

Ansökan handläggs av personuppgiftsombudet. Kontaktpersonen informeras sedan skriftligen om att registret har införts i sjukhusets registerförteckning samt att registrering av uppgifter kan börja.

Personuppgiftslagen (PuL)

Personuppgiftslagen (PUL) är en lagstiftning till skydd för den enskildes integritet. Huvudregeln är att den registrerade ska informeras och samtycka till behandlingen av personuppgifter. Lagen ger också den registrerade rättigheten till kontroll av sina uppgifter.
PUL ställer inte något krav på licens eller tillstånd från Datainspektionen för att få behandla personuppgifter. I stället ansvarar de personuppgiftsansvariga självständigt för att deras behandling av personuppgifter överensstämmer med lagen. För behandling av känsliga uppgifter gäller särskilda regler. Den som bryter mot PUL kan bli skadeståndsskyldig eller dömas till straff.
Den personuppgiftsansvarige är skyldig att anmäla all behandling av personuppgifter till personuppgiftsombud om det finns, annars till Datainspektionen.

Patientdatalagen (PdL)

Patientdatalagen ska öka patientsäkerheten och inflytandet för patienterna. Lagen ställer krav på säkerhet, dokumentation och regler för sekretess och åtkomst. Den gör det möjligt för fler vårdgivare att lättare ta del av en patients journal. Patienterna har ökade möjligheter att införa avvikande mening.

FAX överföring

För faxöverföring av sekretessbelagda uppgifter, t.ex. patientuppgifter, från Södra Älvsborgs Sjukhus (SÄS) gäller nedanstående föreskrifter. Dessa gäller även för de fall överföringen sker med hjälp av datorer som utrustats för faxanvändning. Som huvudregel gäller att sändning och mottagning skall ske på ett sådant sätt att sekretesskyddet för patienten kan upprätthållas. Läs mer i riktlinje ”Fax - Regelverk för att skicka vid SÄS” Dnr:
Undantag från nedanstående regler får endast ske i akuta situationer.

1. Vid sändning av fax ansvarar alltid avsändaren av faxet för att det kommer till rätt mottagare.
   Avsändaren ansvarar också för att mottagaren av faxet på ett enkelt och tydligt sätt ska kunna se vem som är avsändare av faxet.

2. Så långt som möjligt skall förprogrammerade nummer, s.k. kortnummer, användas. Särskilt viktigt är detta när faxmeddelanden sänds till en mottagare där ingen personal finns tillgänglig för att ta emot faxet. Förprogrammerade nummer skall kontrolleras regelbundet så att man är säker på att de är aktuella.

3. Där inte förprogrammerade kortnummer eller motsvarande kan används måste man vara extra noggrann när man slår numret. Vid ett sådant tillfälle skall man vara två personer som kontrollerar att rätt nummer har angetts.

4. I nyare faxarna finns en funktion där inkommande fax inte skrivs ut innan man har angett sin kod på faxens tangentbord. Använd denna funktion för att förhindra att inkommande fax blir liggande utan att någon tar hand om dem.

5. Faxapparatens trafikrapport skall skrivas ut regelbundet och bevaras i två år.

6. Hela patientjournaler och sådana journalutdrag som innehåller särskilt integritetskänsliga uppgifter (t.ex. om könssjukdom, sexliv, psykiatrisk diagnos/tillstånd, tvångsvård) får inte utan väl motiverade medicinska skäl överföras via fax.

7. All medicinsk information skall vara försedd med personidentifikation. Detta för att mottagaren av faxet alltid måste kunna vara säker på vilken person den faxade journalen/journalutdraget handlar om.

8. Faxöverföring av patientuppgifter till mottagare utanför SÄS tar inte bort den vanliga menprövning enligt sekretesslagen.

9. Sändning av journaluppgift per fax innebär rent fysiskt att en kopia skapats av det avsända dokumentet. Enligt journallagen skall detta antecknas i originalakten.