

# VITS-bok – Regelverk till arkitektur för eHälsa i samverkan

Verksamhet  
Information  
Teknik  
Säkerhet

Denna del av VITS-boken avser:

## Informationssäkerhet (S-boken)

- ✓ S-boken sammanställer krav så att projekt och förvaltningsobjekt kan uppfylla de krav som vårdgivarna har att fullgöra avseende infosäkerhet i deras hantering av vårdinformation.
- ✓ S-boken Innehåller krav som vårdgivarna bör ställa på varandra för att uppnå tillräcklig säkerhetsnivå vid nyttjandet av gemensamma tjänster.
- ✓ Målgrupp för S-boken finns beskriven i övergripande VIT(S)-bok

## Innehåll

1	Styrande och rådgivande dokument .....	5
2	Organisatorisk säkerhet.....	7
3	Hantering av tillgångar.....	9
4	Personalrelaterad säkerhet.....	10
5	Fysisk och miljörelaterad säkerhet.....	10
6	Styrning av kommunikation och drift.....	11
7	Styrning av åtkomst .....	11
8	Anskaffning, utveckling och underhåll av informationssystem .....	11
9	Hantering av informationssäkerhetsincidenter .....	12
10	Kontinuitetsplanering .....	12
11	Efterlevnad .....	12

*Denna S-bok är en första utgåva som kommer att kompletteras/revideras utifrån de erfarenheter som användningen av nationella IT-tjänster ger.*

## INLEDNING

Hälso- och sjukvårdsverksamhet är beroende av information för att kunna bedrivas ändamålsenligt. Informationen måste därför hanteras med god informationssäkerhet.

Informationssäkerhet är att säkerställa att information, i alla dess former finns tillgänglig när den behövs, att den är korrekt, att obehöriga inte kan få tillgång till den, och att händelser i hanteringen av informationen kan spåras. En god informationssäkerhet upprätthåller patientintegritet, trygghet för vårdpersonal och bidrar till god och säker vård.

Informationssäkerhet brukar beskrivas utifrån följande fyra egenskaper:

### **Konfidentialitet**

Konfidentialitet avser inte endast sekretess utifrån Offentlighets- och sekretesslagen samt omfattar mer t.ex. en bedömning som tar hänsyn till hur pass känslig en informationsmängd bedöms vara och hur denna bör skyddas.

### **Riktighet**

Information får inte förändras eller gå förlorad, av misstag, genom inverkan av obehörig eller på grund av tekniskt fel. Riktighet innebär att informationen inte ska vara förvanskad, det tar dock inte höjd för att informationen är korrekt i sak.

### **Tillgänglighet**

Information ska kunna användas i förväntad utsträckning, inom önskad tid och av den person som har behov av informationen.

### **Spårbarhet**

Alla aktiviteter skall kunna härledas till en identifierad användare som kan hållas ansvarig för dessa.

För att informationssäkerhet ska kunna bidra till verksamhetsprocessen krävs att man förstår och

S-bokens bidrag till att uppnå eHälsa i samverkan är;

- att bygga ett gemensamt regelverk ska säkerställa att projekt och förvaltningsobjekt möjliggör för vårdgivaren att ta sitt ansvar för informationssäkerhet och personuppgiftsansvar
- att bygga ett gemensamt regelverk som ställer nödvändiga krav på respektive vårdgivare vid nyttjandet av gemensamma tjänster

S-boken bygger på de juridiska grunderna och svensk standard för informationssäkerhet. Det är ett dynamiskt dokument som kommer att utvecklas över tid. I takt med att de nationella tjänsterna utvecklas och tas i bruk kommer det att ställas utökade krav på t.ex. organisation och stödfunktioner. Därför innehåller en del avsnitt vad som behöver regleras men inte hur.

Det går också att säga att informationssäkerhet är förmågan hos en organisation att hantera information så att legala, etiska och verksamhetsmässiga intentioner upprätthålls. Rätt hantering av information bidrar även till en effektiv verksamhet avseende resursanvändning och ekonomi, samt till att upprätthålla en bra arbetsmiljö.

De organisatoriska förutsättningarna för att tillgodose informationssäkerheten i de nationella tjänsterna är komplexa då flera aktörer samverkar.

## 1 Styrande och rådgivande dokument

### 1.1 Rättskällor och lagtolkning

I förteckningen nedan finns uppräknat ett urval av lagar och andra författningar som på olika sätt reglerar informationshanteringen inom hälso- och sjukvården. Det kan röra sig om både övergripande krav och mer specifika krav på informationsutbyte mellan utpekade parter i en utpekad situation. Förteckningen är inte fullständig och varje nationellt projekt behöver inventera vilken lagstiftning och vilka föreskrifter som berör och styr just deras projekt.

När lagar och andra författningar ska tolkas och tillämpas är det viktigt att man känner till några grundläggande principer för lagtolkning. Författningar delas in i lagar, förordningar och föreskrifter. Lagarna beslutas av Riksdagen, förordningarna av Regeringen och föreskrifter av olika myndigheter, tex Socialstyrelsen och Datainspektionen. De viktigaste författningar är grundlagarna, sedan kommer lagar, förordningar och föreskrifter i fallande ordning.

Om det uppstår konflikter vid tolkningen, dvs. olika författningar har motstridigt innehåll finns det tre principer att ta hjälp av:

*Lex Superior* – innebär att en författning högre upp i hierarkin har företräde framför en längre ner. En lag går alltså före en myndighetsföreskrift.

*Lex Specialis* – En specialförfattning har företräde framför en mer allmänt hållen författning. Reglerna i patientdatalagen har inom sitt område företräde framför reglerna i personuppgiftslagen.

*Lex Posterior* – En nyare författning har företräde framför en äldre författning.

### 1.2 Exempel på styrande författningar

- Tryckfrihetsförordningen (1949:105)

Här regleras offentlighetsprincipen, dvs. att offentlig myndighet har skyldighet att lämna ut allmänna handlingar. För privata sektorn däremot föreligger ingen generell skyldighet att lämna ut handlingar.

- Offentlighets- och sekretesslagen (2009:400)

Offentlighets- och sekretesslagen anger vilken information som är sekretessbelagd och alltså undantaget från regeln att myndigheternas allmänna handlingar är offentliga. Sekretess innebär både förbud att röja en uppgift och förbud att lämna ut allmänna handlingar.

- Hälso- och sjukvårdslagen (1982:763)

Hälso- och sjukvårdslagen reglerar hur sjukvården ska bedrivas så att den uppfyller kraven på god och säker vård. Detta innebär bl.a. att den ska vara av god kvalitet och tillgodose patientens behov av trygghet i vården och behandlingen vara lättillgänglig, bygga på respekt för patientens självbestämmande och integritet samt främja goda kontakter mellan patienten och hälso- och sjukvårdsmedarbetaren.

- Tandvårdslagen (1985:125)

Tandvårdslagen anger landstingens och de privata vårdgivarnas skyldigheter inom tandvården. Tandvårdslagen är uppbyggd på samma sätt som hälso- och sjukvårdslagen.

- Patientdatalagen (2008:355)

I patientdatalagen preciseras skyldigheten att föra journal inom hälso- och sjukvården. Lagen ger även möjlighet till sammanhållen journalföring som innebär att vårdgivare via elektroniska system kan ge eller få direktåtkomst till personuppgifter hos en annan vårdgivare.

Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14M) kompletterar lagen med mer konkreta anvisningar.

- Arkivlagen (1990:782)

Anger allmänna riktlinjer för bevarande, gallring och arkivering. Riktlinjer om bevarande/gallring av patientjournaler finns till viss del i patientdatalagen, samt i särskilda bestämmelser som utfärdas av aktuell arkivmyndighet.

- Lagen (2005:258) om läkemedelsförteckning

Styr Apotekens Service behandling av den förteckning där uppgifter om alla receptförskrivna läkemedel, som har hämtat ut på apotek i Sverige, samlas.

- Patientsäkerhetslag (2010:659)

En ny patientsäkerhetslag trädde i kraft den 1 januari 2011 och syftar till att skapa en säkrare vård. Syftet med den nya lagstiftningen är att få ned antalet vårdskador, oavsett om bristerna beror på systemfel hos vårgivaren eller på att vårdpersonalen har begått misstag.

- Personuppgiftslagen (1998:204)

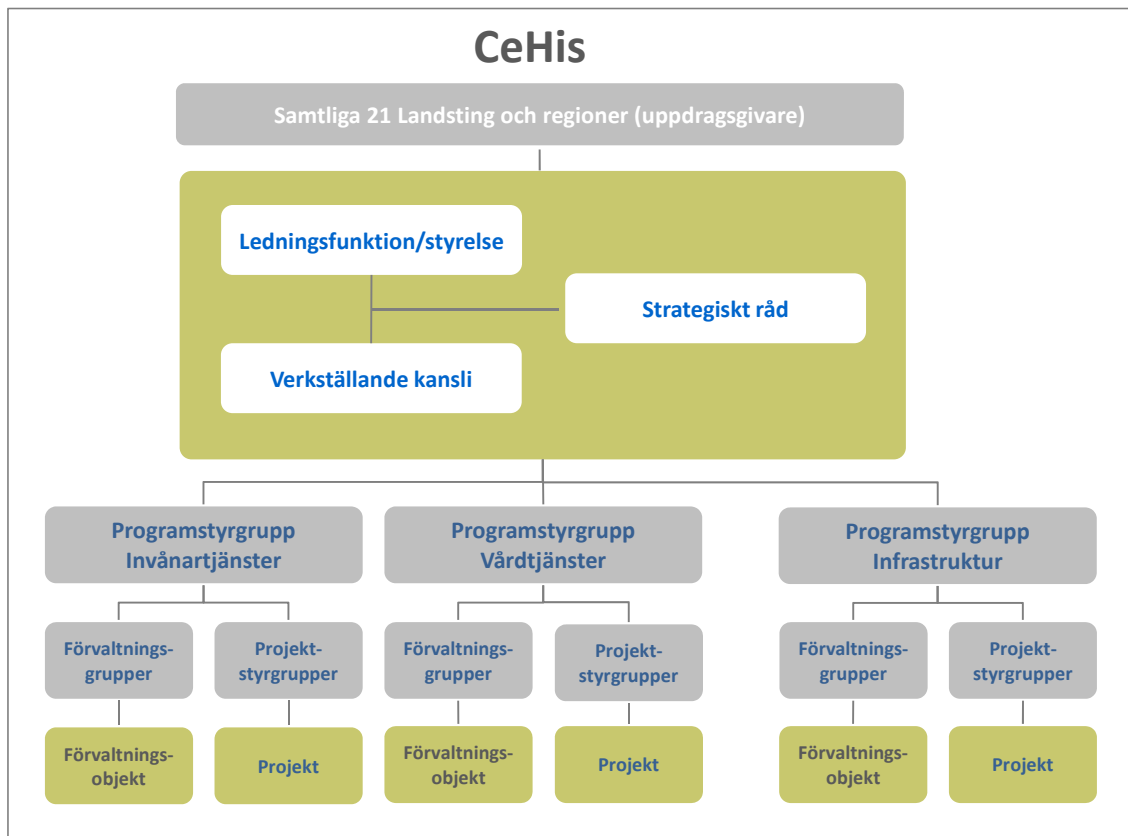
Personuppgiftslagen följer EU:s dataskyddsdirektiv och syftar till att skydda den personliga integriteten. Lagen preciserar villkor för att behandla personuppgifter inom hälso- och sjukvården. Genom patientdatalagen införs en laglig grund för att hantera administration och dokumentation inom vården med hjälp av IT-stöd. Lagen fordrar inte samtycke.

### 1.3 Andra styrande dokument

Utöver författningarna ovan ger Datainspektionen ut allmänna råd, Socialstyrelsen har tidigare gett ut allmänna råd men gör det inte längre. Trots att de allmänna råden inte är bindande får de ses som styrande dokument eftersom följsamhet till dessa i flera fall är näst intill nödvändigt för att vårdgivaren ska anses uppfylla övriga författningar. Socialstyrelsen ger även ut handböcker inom vissa områden.

En särskild typ av styrande dokument är rapporten PDLiP1 som tagits fram av CeHis expertgrupp AL-S. Detta dokument är inte någon rättskälla enligt definitionen ovan men är ändå styrande för landstingen eftersom samtliga landsting har antagit dokumentet och beslutat att det ska vara styrande vid informationshanteringen.

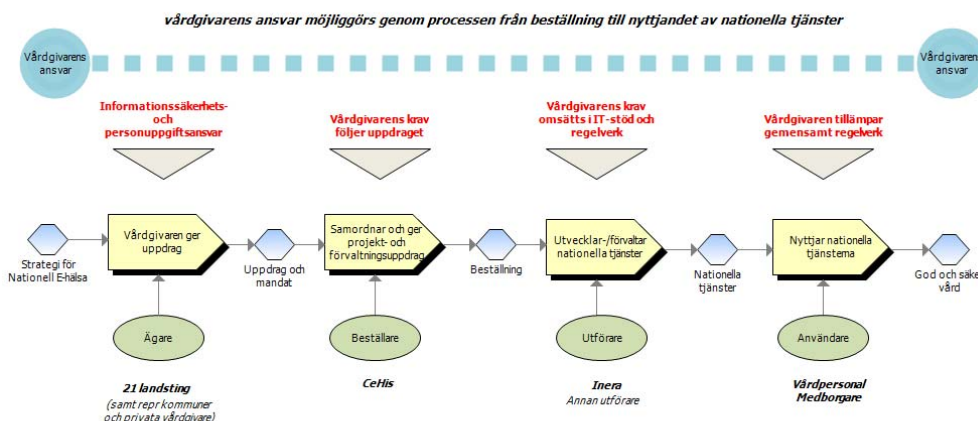




## 2.2 Vårdgivarens informationssäkerhets- och personuppgifts ansvar

Vårdgivaren har informationssäkerhetsansvar och personuppgiftsansvar för hos vårdgivaren upprättad information.

Nedanstående bild visar hur detta ansvar säkerställs i de till användarna levererade nationella tjänsterna.



När vårdgivarna ger mandat till CeHis att beställa nationella tjänster medför detta ett ansvar för CeHis att ställa säkerhetskrav på dessa tjänster. För att få fram nationella tjänster beställer och samordnar CeHis projekt och förvaltningsobjekt. CeHis använder utförare, huvudsakligen Inera, för att realisera dessa projekt och förvaltningsobjekt och måste därför ställa informations-säkerhetskrav även på utföraren. Vid behandling av personuppgifter måste dock vårdgivaren teckna personuppgiftsbiträdesavtal med utföraren och eventuellt deras underleverantörer.

Informationssäkerhetskraven enligt ovan omfattar bland annat att:

- författningskrav och utarbetade regelverk ska följas
- informationsklassificering ska genomföras och skyddsnivåer specificeras utifrån detta
- riskanalyser genomförs utifrån informationsklassificering
- förvaltningsplan upprättas
- avbrottsplan för IT-tjänsterna utarbetas
- förteckning förs över vilken information som behandlas av IT-tjänsten och tjänstens syfte

Tillsynsmyndigheter ställer krav på vårdgivarna. I och med detta ställs krav på de nationella tjänsterna. Då olika aktörer ingår i en gemenskap gäller att varje aktör uppnår den gemensamt överenskomna säkerhetsnivån.

### 3 Hantering av tillgångar

Information och data som skapas, inhämtas, bearbetas, distribueras och lagras är en kritisk tillgång för hälso- och sjukvårdsverksamheten. En korrekt kunskap om de nationella tjänsterna och dess information är därför nödvändigt för att bedriva ett effektivt informationssäkerhetsarbete.

Projekt och förvaltningsobjekt ska ha gjort informationsklassificering enligt i RIV-metoden (se [informationssakerhet.se](http://informationssakerhet.se) för mer information). Utifrån informationsklassificeringen ska informationen ha rätt nivå av tillgänglighet, skydd mot obehörig insyn och förvanskning. Dessutom ska behandlingen av informationen vara spårbar.

Riskanalys ska genomföras och stödja de nationella tjänsternas säkerhetsarbete och användas som ett verktyg för att analysera risker utifrån potentiella hot. Riskerna bedöms utifrån hur stor sannolikheten är att hoten realiserar och konsekvenserna av detta. Riskanalyserna ger underlag för att fastställa de skyddsåtgärder som behöver införas och ska utmynna i prioriterade åtgärdsplaner för att hantera riskerna. Åtgärdsplanerna ska vara balanserade, dvs. skyddsåtgärder som väljs ska stå i proportion till de risker som varje informationsmängd är utsatt för samt informationens värde.

Hantering av information såsom t ex utlämning, rättning och radering är vårdgivarens ansvar, men kan utföras av annan part på uppdrag av vårdgivaren. Informationen i de nationella tjänsterna måste kunna hanteras på ett sådant sätt att gallring och arkivering kan ske utifrån vårdgivarnas krav.

Varje vårdgivare ansvarar för sin information. Vid lagring i gemensam databas måste informationen märkas med ansvarig organisation. Bearbetning kan ske i gemensam databas men var och en har ansvar för sin informationsmängd. Varje informationsägare, personuppgiftsansvarig, ska endast ha tillgång till sin information i databasen, om inte förutsättningarna för sammanhållen journalföring är uppfyllda,

En företeckning över de nationella pågående projekt och förvaltningsobjekt som CEHIS driver finns på hemsidan [www.CEHIS.se](http://www.CEHIS.se).

## 4 Personalrelaterad säkerhet

Det är vårdgivarens och utförarens ansvar att ha kontrollrutiner och tillräckliga säkerhetsrutiner avseende anställda, leverantörer och utomstående användare. HSA och SITHS är exempel på regelverk som stödjer den personalrelaterade säkerheten.

## 5 Fysisk och miljörelaterad säkerhet

Fysisk säkerhet syftar till att skydda lokaler, utrustning och informationskapital. Brister i fysisk säkerhet kan medföra att de logiska säkerhetsskydden sätts ur spel.

Nivån på det fysiska skyddet ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad. Utrustning som är känslig i sig själv eller behandlar känslig information, ska placeras och hanteras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.

Kritiska IT-system och informationstillgångar ska inrymmas i säkra utrymmen, omgärdade av skalskydd, med lämpliga tillträdesspärar och -kontroller.

## 6 Styrning av kommunikation och drift

En förutsättning för att de flesta informationssystem ska fungera är den underliggande infrastrukturen. Varje enhet måste kunna lita på att nödvändiga resurser är tillgängliga vid behov. För att säkerställa och övervaka detta är ändamålsenlig drift en annan förutsättning för väl fungerande informationssystem.

Förvaltningsmodell ska användas och dessutom ska det finnas ett avtal för varje objekt med preciserat ansvar inklusive gränssnitt för ansvar mellan respektive vårdgivare och utföraren med underleverantör.

I dessa avtal kan nedanstående ingå:

- SLA mellan vårdgivare och utförare.
- Beskrivning av säkerhetskopiering
- Reglering av kundtjänst
- Reglering av övervakning
- Bestämmelse att informationsutbyte ska ske enligt nationellt överenskomna lösningar
- Dokumenterad ändringshantering
- Krav på systemdokumentation

## 7 Styrning av åtkomst

Åtkomst till information och informationsbehandlingsresurser ska styras av legala-, verksamhets- och säkerhetskrav. Det krävs reglering för att säkerställa att behöriga användare får åtkomst till en viss informationsmängd, samtidigt som obehöriga användare ska förhindras åtkomst till informationen. Bedömning av vilka säkerhetsåtgärder som behövs är beroende bl.a. av vilka uppgifter som behandlas.

Systemet ska kunna kontrollera nyttjandet av en tjänst eller ett system så att endast de som behöver uppgifterna för sitt arbete har tillgång till dem. Till detta ska det finnas rutiner för tilldelning och kontroll av behörigheter.

Regler för åtkomst till patientuppgifter är beskrivet i dokumentet Patientdatalagen i praktiken, etapp 1.

Förtydligande av krav på loggning framgår av råd ”Krav på loggning, modellering av logginformation (från Patientdatalagen i praktiken etapp 2)” samt råd ”Kontroll av åtkomst till patientuppgifter” (loggranskning).

## 8 Anskaffning, utveckling och underhåll av informationssystem

Säkerheten ska vara en integrerad del av informationssystemet och beaktas redan vid anskaffning och utveckling.

För nationella projekt ska en fastställd projektmodell och förvaltningsmodell användas.

RIV-metoden ska användas vid utveckling av de nationella tjänsterna. Utifrån RIV-metoden tas sedan informationssäkerhetskraven fram.

Utförlig system-, användar- och driftdokumentation ska framställas i utvecklingsprojektet. Vid systemanskaffning ska denna dokumentation tillhandahållas av utföraren. Fastställda rutiner ska finnas som säkerställer att dokumentationen uppdateras vid förändringar av systemet.

## 9 Hantering av informationssäkerhetsincidenter

Informationssäkerhetsincidenter ska rapporteras så att korrigerande åtgärder kan åtgärdas i tid. Formella rutiner bör finnas för händelsehantering och eskalering.

Både vårdgivare och utförare med underleverantörer ska ha en organisation och metoder för hantering av informationssäkerhetsincidenter gällande de nationella tjänsterna. För respektive nationell tjänst ska incidenthanteringen regleras mellan vårdgivare och utförare.

## 10 Kontinuitetsplanering

Kontinuitetsplanering i verksamheten ska motverka avbrott i en organisations verksamhet och skydda kritiska verksamhetsprocesser från allvarliga fel.

Vårdgivare ska ha kontinuitetsplanering som utgår ifrån verksamhetens behov utifrån informationsklassningen. Kontinuitetsplaneringen ska inkludera reservrutiner. Dialog ska finnas med utföraren angående vårdgivarens kontinuitetsplanering .

Utförare och/eller driftleverantörer ska ha avbrottsplaner som syftar till att återställa driften av den nationella tjänsten. Avbrottsplan ska vara känd för vårdgivaren och avbrott ska kunna kommuniceras mellan vårdgivare och utförare på flera olika sätt.

## 11 Efterlevnad

Alla aktörer ska följa gällande författningar, avtalsförbindelser och andra säkerhetskrav.

Externa tillsynsmyndigheter genomför revisioner via tillsyner som sker mot vårdgivare. Detta ställer krav både på vårdgivarna och på de nationella tjänsterna.

Inom CeHis verkställandekansli genomför Arkitekturledningen granskning av projekt och förvaltningsobjekt

Det bör även finnas en möjlighet för vårdgivare och utförare att genomföra revision av varandra för att säkerställa att rätt kvalitet och säkerhet uppnås i de nationella tjänsterna.

Vid otillåten behandling av personuppgifter är det alltid den personuppgiftsansvariga som drabbas av ett ev. skadeståndsanspråk.