



Checklista

Säkerhetslösning för Pascal



Innehållsförteckning

1. Inledning	3
2. Inloggning/autentisering i Pascal	3
3. Säkerhetstjänsten	4
4. Vad är HSA	4
5. Vad är SITHS	4
6. På vilket sätt fungerar SITHS och HSA ihop	4
7. Adresser för åtkomst till Pascal	4
8. Checklista med kommentarer för anslutning till Pascal	6
9. Checklista för anslutning till Pascal	18



CHECKLISTA - SÄKERHETSLÖSNING FÖR PASCAL

1. Inledning

Detta dokument är en **checklista** som ska vara en hjälp till införandeansvariga i region, kommun och privata vårdgivare för att möjliggöra tillgång till Pascal. Här beskrivs vad som ska göras, medan det i refererade dokumenten förtydligar hur man gör det.

För att en person skall kunna använda Pascal krävs att hen finns upplagd i HSA. Det krävs också att personen är kopplat till ett (eller flera) medarbetaruppdrag, samt att vissa specifika uppgifter om person och organisation är angivna.

2. Inloggning/autentisering i Pascal

För autentisering (d.v.s. inloggning och identifiering av användaren) används SITHS-kort eller SITHS eID.

Pascal har möjliggjort 3 olika inloggningssätt för användare:

1. Inloggning med **SITHS-kort** eller **SITHS eID-kort** med kortläsare via **NET iD-klient** kortläsarprogramvara
2. **SITHS eID-kort** med kortläsare via **SITHS eID Windowsklient** kortläsarprogramvara
3. **SITHS eID** via **SITHS eID Mobilklient** (på samma enhet eller på annan enhet)

För detaljer se dokumentet "Teknisk anslutning Pascal"

(<https://inera.atlassian.net/wiki/spaces/OIP/pages/2360541715/Teknisk+anslutning>)

OBS!

Net iD-stödet efter 2023-06-30

Inera kommer sluta att tillhandahålla support för Net iD Enterprise i samband med att Ineras nuvarande avtal löper ut 2023-06-30. Viktigt att notera är att Inera efter 2023-06-30 ej kan säkerställa att SITHS eID-app för Windows kan samexistera med Net iD Enterprise.

Överväg därför SITHS eID och inloggningssätten 2 och 3 ovan

Alla personer måste vara upplagda i HSA med rätt egenskaper.



3. Säkerhetstjänsten

Nationella IT-lösningar för vård och omsorg måste garantera säkerhet, integritet och sekretess. Användare måste kunna identifieras och tillgång till information anpassas efter användaren. Detta är krav som den nya Patientdatalagen ställer. Det är i detta sammanhang som Säkerhetstjänsternas IdP kommer in. Tjänsterna hjälper till att kontrollera att endast rätt person får tillgång till rätt information. För åtkomst till Pascal används SITHS för att kontrollera att jag är jag och HSA för att tala om vad jag får göra.

4. Vad är HSA

HSA är en elektronisk katalog som innehåller grundläggande uppgifter om anställda och deras organisatoriska tillhörighet, men också uppgifter som beskriver den anställdes roller och uppdrag inom vård och omsorg. När en person behöver ta del av till exempel vårdinformation från ett vårdsystem används uppgifterna i HSA för att kontrollera att personen i fråga verkligen är anställd inom vård/omsorg samt har en roll/uppdrag. Därefter kan personen ta del av den efterfrågade informationen som han/hon är behörig till. Ansvaret att hålla HSA uppdaterad åvilar verksamheten och dess lokala HSA-administratörer.

5. Vad är SITHS

SITHS är en tjänstelegitimation i form av ett plastkort som innehåller elektroniska certifikat som bland annat används för att kunna logga in i olika IT-system.

Organisationen som utfärdar legitimationen kan, förutom elektronisk ID-handling, förse kortet med text och grafik (namn, personnummer, foto, namnteckning, logotyp, med mera). Certifikaten möjliggör så kallade "två-faktors-autentisering" vilket betyder att det inte bara räcker med att ha kortet som bevis för sin identitet, kortägaren måste också känna till en PIN-kod, för att identiteten ska anses vara bevisad.

6. På vilket sätt fungerar SITHS och HSA ihop

Det elektroniska certifikatet som finns på SITHS-kortet bygger på uppgifter som finns i HSA-katalogen. Du kan alltså inte få ett SITHS-kort om du inte finns med i HSA. När en person "loggar in" med hjälp av SITHS-kortet så görs först en kontroll av att certifikatet fortfarande är giltigt. Är det giltigt så söks personen med det aktuella certifikatet upp i HSA-katalogen. Därefter avgör personliga egenskaper tillsammans med medarbetaruppdraget i HSA-katalogen inom vilket område och vilken information personen har rätt att ta del av.

7. Adresser för åtkomst till Pascal

Åtkomst till Pascal kan ske både från sjunet och internet på följande adresser:



Sjunet: <https://siths.eordinationpascal.sjunet.org> (alt 1 i kap 2)
<https://eid.eordinationpascal.sjunet.org> (alt 2 och 3 i kap 2)

Internet: <https://siths.eordinationpascal.se> (alt 1 i kap 2)
<https://eid.eordinationpascal.se> (alt 2 och 3 i kap 2)



8. Checklista med kommentarer för anslutning till Pascal

Syftet med checklistan är att ge de införandeansvariga i region, kommun och privata vårdgivare en hjälp att kontrollera att organisationen har utfört de aktiviteter som behöver genomföras för att få tillgång till Pascal. Till varje punkt i checklistan finns kommentarer angivna för att ge en översiktlig information om respektive punkt. Till vissa punkter finns även hänvisning till dokument som ger en mer utförlig information om punkten i fråga.

För ytterligare information om Pascal finns en [Handbok](#) för användare framtagen, vilken innehåller fördjupning och utbildning i verket.

Ansluten till HSA

Direktanslutning till HSA: Din verksamhet har ansökt om anslutning samt tecknat avtal direkt med Inera.

Tredjepartanslutning till HSA via region eller kommun: Din verksamhet har ansökt om anslutning samt tecknat avtal med en organisation som har en direktanslutning till HSA.

För mer information, se [Anslutning till HSA](#).

Tredjepartanslutning till HSA via privat ombud: Din verksamhet har ansökt om anslutning samt tecknat avtal via privat ombud. För mer information, se [Tredjepartanslutning till HSA](#).

Ansluten till SITHS

Direktanslutning till SITHS: Din verksamhet har ansökt om anslutning samt tecknat avtal direkt med Inera.

Tredjepartanslutning till SITHS via region eller kommun: Din verksamhet har ansökt om anslutning och tecknat avtal med en organisation som har en direktanslutning till SITHS, ett så kallat ombud för SITHS.

För mer information, se [Anslutning till SITHS](#).

Tredjepartsanslutning till SITHS via privat ombud: Din verksamhet har ansökt om anslutning samt tecknat avtal via privat ombud. För mer information se, [Tredjepartanslutning via SITHS-ombud](#).



SITHS-kort och kortläsare beställda

SITHS-kort beställs av Er lokala SITHS-organisation.

Systemkrav och rekommendationer

Tillbehör, såsom kortläsare finns ofta i tangentbord eller som extern kortläsare. Godkända kortläsare finns att köpa från de flesta datorleverantörer.

För mer information avseende systemkrav hänvisas till dokumentet [Systemkrav och rekommendationer för åtkomst till Pascal](#).

Krav/rekommendationer på operativsystem och webbläsare uppfyllda

Följande kombinationer (X) av operativsystem, webbläsare och Net iD stöds och supportas av Inera och Secmaker **fram till 2023-06-30**. Javascript och Cookies ska vara påslaget (enable) i webbläsarna nedan.

Operativsystem och webbläsare	Net iD			
	6.5.x	6.6.x	6.7.x	6.8.0
Windows 10				
IE 11 (32 bit)	ESK	X*	X*	ESK
Edge (32 bit)	X**	X**	X**	X**
Chrome	X**	X**	X**	X**
Windows 8.1 Modern UI ***	Paketering: SITHS1901***			
IE 11 (32 bit)	ESK	X**	X**	ESK
Chrome	X**	X**	X**	ESK

* **OBS!!** När SITHS-kortet rycks ut i denna kombination så kan meddelandet "Ett problem med webbsidan fick Internet Explorer att stänga och öppna fliken igen" erhållas och man kommer till sidan "Fel vid inloggning med SITHS-kort". Detta kan åtgärdas genom att inaktivera den automatiska återställningen efter krasch. Detta görs under Internetalternativ – Avancerat – Webbsökning.

ESK = Ej Supporterad Kombination
X = Stöds

** **OBS!** Paketering SITHS1901 måste användas. Tänk på att denna paketering inte stödjer utloggning ur Pascal via utdragning av SITHS-kortet. Därför ska man alltid använda knappen **Logga ut** i Pascal vid utloggning och därefter stänga sin webbläsare vilket är den primära utloggningen som alltid bör användas.

*** Modern UI är det läge/användargränssnitt som introducerades i och med lanseringen av Windows 8. Modern UI är standardgränssnittet i 8.1 och är speciellt anpassat för mobila enheter t ex. surfplattor/tablets.

Andra kombinationer än ovan kan fungera men stöds och supporteras inte av Inera & Secmaker.



Om man har en annan kombination så ska man testa så att in- och utloggning sker på ett korrekt sätt. Om så inte sker ska man uppdatera sin konfiguration enligt matrisen ovan.

Vi rekommenderar att man markerar i webbläsarens inställningar att vid inloggning visa certifikat endast då fler än ett certifikat finns på SITHS-kortet enligt följande:

Välj **Internetalternativ** – fliken **säkerhet** - Klicka på **Betrodda platser** och sedan på knappen **Anpassad nivå**. Markera **Aktivera** under rubriken **”Fråga inte efter val av klientcertifikat när det bara finns ett certifikat”**

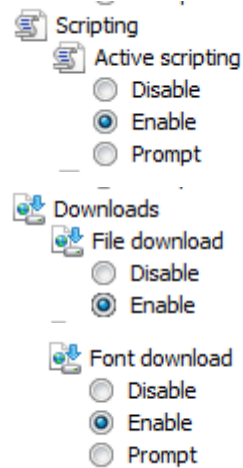
Anpassa säkerhetsnivån i webbläsaren

För att SITHS-korthantering och SingleSignOn ska fungera som tänkt, ska aktuella domäner/ siter som säker inloggning sker mot finnas inlagda som "Betrodda platser" i Internet Explorer.

Lägg till följande domäner under **Internetalternativ - Säkerhet – Betrodda platser – Platser** i Internet Explorer:

- https://*.eordinationpascal.se
- https://*.inera.se
- https://*.sjunet.org

Säkerhetsnivån skall vara mellan. Man kan ändra säkerhetsnivån, men inte parametrarna "Active scripting", "File download" och "Font download" som måste vara satta till enable.





Krav/rekommendationer på Net iD uppfyllda

Vi stödjer att ni har **Net iD** installerad som CSP-programvara (programvara för att läsa SITHS-kort) och **SITHS eID Windowsklient** kortläsarprogramvara

Vi stödjer Net iD version enligt matris ovan **fram till 2023-06-30**. Se vidare kap 2

Om organisationen har en direktanslutning till SITHS (har avtal med Inera) så finns det på SITHS projektplats installationspaket att ladda ner som innehåller rätt inställningar i Net iD (enbart RA-organisationen, Registration Authority har tillgång till detta). Är man ansluten till SITHS via en annan organisation (tredjepartanslutning), så kan denna organisation tillhandahålla installationspaket för Net iD.

I vissa fall kan man ha gjort lokala anpassningar av Net iD. Den information (beroende på version av NetId) som behöver finnas i **Net iD:s konfigurationsfil (iid.cfg) under program/Net iD** alternativt Windows registry för att nedstängning av webbläsaren ska fungera är:

Namn	Typ	Data
(Standard)	REG_SZ	(värde har ej angetts)
Applications	REG_SZ	iexplore.exe;firefox.exe;chrome.exe
Ask	REG_SZ	0
Enable	REG_SZ	1
LogonApplications	REG_SZ	iexplore.exe;firefox.exe;chrome.exe
TabNames	REG_SZ	TabWindowClass;MozillaUIWindowClass;MozillaWindow...

[NetControl]

Applications=iexplore.exe; iidweb.exe

Ask=0

Enable=1

Det kan finnas andra sätt att få nedstängning av webbläsaren att fungera än som beskrivits ovan, men då får man själv genomföra tester så att nedstängning av sessionen sker på ett korrekt sätt när SITHS-kortet rycks ur kortläsaren.

Det är dock viktigt att understryka att den primära utloggningen ur Pascal är att alltid använda knappen Logga ut.



Brandväggar öppnade

För att komma åt **Pascal** krävs att följande brandväggar är öppna, se nedan.

Sjunet

IP-adress	Url	Port
81.89.154.161	https://siths.eordinationpascal.sjunet.org	443
82.136.182.2	https://idp.inera.se	443
81.89.154.161	https://eid.eordinationpascal.sjunet.org	443

Internet

IP-adress	Url	Port
164.40.178.0	https://siths.eordinationpascal.se	443
82.136.182.2	https://idp.inera.se	443
164.40.178.0	https://eid.eordinationpascal.se	443

OBS! kontrollera att adressen ovan inte spärras i någon generell produkt för internetfiltrering (typ Bluecoat).

IdP (Identity Provider) är tillgänglig på både Sjunet och Internet med samma hostname. Detta hostname resolver olika IP-adresser beroende på vilket nät/DNS som används. Inera IdP är tillgänglig från både Internet och Sjunet med samma instans och domän. De IP-adresser som används av tjänsten finns i en range som länge funnits endast på Sjunet så i många fall kan brandväggar (443) behöva öppnas mot angivna adresser för de klienter på nätverk som ska nå Pascal. Det beror på hur er organisation med klienterna routar 82.136.182.0/24 nätet. Organisationer med både internet- och sjunetanslutning behöver för en fullständig anslutning över Sjunet - för både DNS-uppslag och IdP-trafik - ett extra steg. För klienter som har DNS-uppslag för både sjunet och internetdomäner adderas en s.k. Conditional Forward i den DNS lösning som används av er idag (som troligen redan har en sådan för sjunet.org). Utan detta finns risk att trafik mot IdPn går över internet när anslutningen är tänkt att vara



över Sjunet, och detta kan t ex uppmärksammas först när internetanslutningen får problem. Förslagsvis valideras vägvalen som går från klient mot respektive miljö med tracert och/eller nslookup. Vid validering kan en rensning av eventuell DNS cache behövas ("ipconfig /flushdns" på Windows).

Dessutom behövs följande **revokeringsadresser** vara öppna:

CA v1

För att komma åt nya spärrar/AIA-lokationer så får följande adresser inte vara blockerade:

Internet:

http://ocsp1.siths.se (IP 194.237.208.174 och 194.237.208.174)

http://aia.siths.se (IP 194.237.208.239 och 194.237.208.239)

http://crl1.siths.se (IP 194.237.208.239 och 194.237.208.239)

Port 80

Sjunet:

http://ocsp2.siths.sjunet.org (IP 82.136.160.42)

http://aia.siths.sjunet.org (IP 82.136.160.44)

http://crl2.siths.sjunet.org (IP 82.136.160.44)

Port 80

Brandväggar måste också öppnas för att HSA- och SITHS-organisationen ska komma åt HSA Admin och SITHS Admin. Detta görs av nätverkstekniker i samband med tjänsternas införande.

- Rekommendationer på Kortläsare och drivrutin uppfyllda

Vissa kortläsare med dess drivrutin kan ibland inte registrera att SITHS-kortet har ryckts ur kortläsaren. Det innebär att Net iD inte upptäcker att något har hänt och följaktligen inte stänger ner sessionen.

Vi rekommenderar därför att ni utgår från Cygates eller Secmakers [kortläsarbroschyr](#), som innehåller kortläsare som fungerar bra. Det är också viktigt att man använder den senaste drivrutinsversionen från tillverkaren. Använd **inte** Microsofts generiska drivrutiner.



Andra läsare kan också fungera bra men var noga med dess drivrutiner.

I båda dessa fall så bör man testa så att kortläsaren och dess drivrutin fungerar korrekt, se stycket om funktionstest av SITHS-kort och dess kortläsare nedan.

När man installerar drivrutiner för olika kortläsare uppmärksammar man sällan att vissa installeras med strömspar PÅ medan andra installeras med strömspar AV. Det har visat sig att strömsparfunktionen kan ställa till med en del märkliga bieffekter i applikationer som pollar efter kort på ett visst sätt. **Ta därför för vana att stänga av strömsparfunktionen för kortläsaren om du får problem.**

Utskrift av "Receptutskrift Pascal" i Pascal fungerar med Adobe Reader version 9 eller senare. Tidigare versioner kan fungera men stöds inte av Inera och eHälsomyndigheten. Om man har en tidigare version än Adobe Reader 9 får man själv testa och validera att utskrift av "Receptutskrift Pascal" sker på ett korrekt sätt.

För information och frågor gällande tunna klienter gäller följande rekommendationer:

1. Kontrollera om supportavtal finns med leverantören/tillverkaren av plattformen.
2. Kontrollera om det finns eget avtal med Secmaker avseende Net iD.



Om supportavtal finns enligt ovan, så vänd er i första hand till dessa för information och support.

3. Om man inte har några supportavtal eller får hjälp enligt ovan kan man via mail, vända sig till Ineras kundservice, support@inera.se, för hjälp och vidare rådgivning.

Rekommendation på pdf-läsare uppfyllda

Tunna klienter fungerar korrekt
(Gäller enbart om man har tunna klienter)



- | | |
|---|--|
| <input type="checkbox"/> Datorkrav/rekommendationer uppfyllda | <p>Kontrollera att datorn uppfyller ovanstående systemkrav och rekommendationer.</p> <p>Kortläsare och senaste drivrutin ska vara installerad på Dator.</p> <p>Net iD ska vara installerad på Dator.</p> |
| <input type="checkbox"/> Användare erhållit SITHS-kort | <p>Kontrollera att användare har erhållit SITHS-kort och kodkuvert.</p> |
| <input type="checkbox"/> Funktionstest av SITHS/kortläsare utförd | <p>Funktionstest av SITHS-kort och dess kortläsare kan ske på följande sätt:</p> <ol style="list-style-type: none">1. Anslut kortläsare till datorn och sätt i SITHS-kortet i kortläsaren.2. Leta upp Net iD genom att klicka på Start  och därefter Alla Program. Klicka på Net iD-mappen och därefter på Administration eller Högerklicka på Net iD-ikonen  och därefter på Administration om den finns på datorns skrivbord. Då visas ett Net iD-fönster där alla certifikat som finns på SITHS-kortet visas.3. Ryck ur SITHS-kortet ur kortläsaren. Då ska alla certifikat som finns på SITHS-kortet försvinna från Net iD-fönstret. Om så inte sker så är det fel på kortläsaren och/eller dess drivrutin.4. Testa ditt SITHS-kort, certifikat och pinkoder på Ineras testsida.5. Testa ditt SITHS-eID, certifikat och pinkoder på https://test.idp.inera.se/ |



Lokal support etablerad

Lokalt kunskapsstöd för Pascal ska finnas tillgängligt. Det lokala kunskapsstödet (supporten) kan vid behov vända sig till Nationell support.

För mer information om vilket ansvar det lokala kunskapsstödet (supporten) har, se dokument [Ansvar för lokal support](#).

Användare registrerad i HSA

För mer information avseende registrering av användare i HSA använd dokumentet [Införandestöd - Säkerhetslösning för Pascal](#). För en mer utförlig beskrivning hur man lägger in attributen i HSA hänvisas till dokumentet [Handbok för HSA-administratörer](#).

Vårdgivare och vårdenhet registrerad

I HSA Admin får endast Huvudansvarig och Central admin markera att en enhet är **vårdgivare** eller **vårdenhet** samt ange vem som är **verksamhetschef** för den aktuella vårdenheten (Verksamhetschefen måste vara upplagd i HSA, men behöver inte ha SITHS-kort). Likaså är det endast Huvudansvarig och Central admin som får ange vilka enheter som tillhör en vårdenhet.

Vårdgivare och vårdenhet kan i vissa fall ligga på samma nivå.

Registrerat organisationsnummer för aktuell vårdgivare

Organisationsnummer behöver finnas registrerat på de objekt som ska definieras som vårdgivare. Definieras i attributet **Org.nummer** (orgNo) i formuläret Enhet i HSA Admin.

Registrerad adressinformation för aktuell vårdenhet

Adressinformationen behövs för att kunna spåra vem som fått åtkomst till eHälsomyndigheten. Det är postadressen och postnummer där verksamheten bedrivs som måste registreras. Detta görs i attributet **Postadress** (postalAddress) i formuläret Adresser i HSA Admin och i attributet **Postnummer där verksamheten bedrivs** (postalCode) i formuläret Kontakt i HSA Admin.



- | | |
|---|---|
| <input type="checkbox"/> Registrerat telefonnummer för aktuell vårdenhet | Telefonnummer till vårdenheten där verksamheten bedrivs, vilket definieras i attributet Direkttelefon (telephoneNumber) i formuläret Kontakt i HSA Admin. |
| <input type="checkbox"/> Registrerad arbetsplatskod för aktuell vårdenhet | <p>Arbetsplatskod¹ (unitPrescriptionCode) registreras i formuläret Enhet i HSA Admin.</p> <p>Arbetsplatskod krävs av Förskrivare för att kunna fakturera kostnaden för läkemedel till rätt kostnadsställe och för att patienten ska få tillgodogöra sig läkemedelsförmån.</p> <p>Finns det flera arbetsplatskoder angivna på vårdenheten eller de enheter som kopplats till vårdenheten så kommer användaren få möjligheter att välja vilken arbetsplats/kod som ska användas vid respektive förskrivning.</p> <p>OBS! Arbetsplatskod som registreras måste vara giltig i ARKO (Arbetsplatskodsregistret).</p> |
| <input type="checkbox"/> Medarbetaruppdrag definierat | <p>Medarbetaruppdraget ska ha syfte "Vård och behandling".</p> <p>Samma medarbetaruppdrag kan användas för flera olika tjänster och det är önskvärt att man återanvänder redan befintliga medarbetaruppdrag där så är möjligt.</p> <p>Man kan alltså använda ett redan definierat medarbetaruppdrag som har Syftet "vård och behandling".</p> <p>Om vårdenheten saknar ett medarbetaruppdrag med syfte "Vård och behandling" måste ett nytt sådant skapas.</p> |

¹ Det är regionerna som hanterar och distribuerar arbetsplatskoder, även för kommuner och privata vårdgivare. Detta görs av respektive regions s.k. ARKO-administratör. För att komma i kontakt med administratören inom er region kan ni antingen fråga efter ARKO-administratören via regionens växel alternativt ta kontakt med eHälsomyndighetens supportfunktion via telefon 0771-766 200 eller e-post registrator@ehalsomyndigheten.se.



- | | | |
|--------------------------|---|--|
| <input type="checkbox"/> | Användare registrerad | Registreras med: Tilltalsnamn (givenName, gn)
Mellannamn (middlename)
Efternamn (sn, surName)

Dessa uppgifter hämtas från befolkningsregistret genom att ange Personnummer när man skapar Person i HSA Admin. |
| <input type="checkbox"/> | Användare kopplad till medarbetaruppdrag | Förskrivare samt personer som tar del av förskrivningen och administrerar läkemedel måste vara kopplade till ett medarbetaruppdrag, definierat enligt ovan. Registreras i formuläret Tilldela medarbetaruppdrag i HSA Admin. |
| <input type="checkbox"/> | Legitimerad yrkesgrupp angiven* | Registreras i attributet Leg yrkesgrupp (hsaTitle) i formuläret Anställning/uppdrag i HSA Admin. |
| <input type="checkbox"/> | Befattning angiven (enbart för visning av receptutfärdare, ej krav) | Registreras i attributet Befattning (paTitleName), (paTitleCode) i formuläret Anställning/ uppdrag i HSA Admin. |
| <input type="checkbox"/> | Förskrivarkod*/gruppförskrivarkod angiven | Personlig förskrivarkod registreras i attributet Förskrivarkod (personalPrescriptionCode) i formuläret Anställning/uppdrag.
Gruppförskrivarkod registreras i attributet Gruppförskrivarkod (hsaGroupPrescriptionCode) i formuläret Anställning/uppdrag. |
| <input type="checkbox"/> | Kontroll av HSA-information | HSA huvudadministratör kan kontrollera sin HSA-information för Pascal via ett kontrollverktyg som finns i HSA – portalen, https://hsahotell.carelink.sjunet.org/hsaportalen/ . |

* För en mer utförlig beskrivning/information om legitimerad yrkesgrupp, befattning och förskrivarkod, **se kapitel 2.3 "Steg 3 - Användarroller Pascal"** i dokumentet [Införandestöd för Pascal säkerhetslösning](#).



Observera att uppgift om "Legitimerad yrkesgrupp" och "Förskrivarkod", samt uppgift om "Specialitet", som registreras i HSA måste överensstämma med uppgifterna om personen i Socialstyrelsens register över hälso- och sjukvårdspersonal, HOSP.

Det finns en mängd olika typer av Förskrivare som var och en kräver olika uppgifter i HSA-katalogen. Uppgifter såsom Legitimerad yrkesgrupp och personliga förskrivarkoder stäms vid anställning av med Socialstyrelsen enligt Er organisations rutin och kan därefter uppdateras kontinuerligt genom kontroller mot Socialstyrelsens register för hälso- och sjukvårdspersonal (HOSP)². Detta görs av organisationens HSA huvudadministratör via den så kallade HSA-portalen och kräver att sökning och korrigering av felaktiga uppgifter initieras manuellt men sedan uppdateras automatiskt. HSA-administratören måste vara uppmärksam på att gruppförskrivarkoder rapporteras som fel/avvikelser. Detta innebär att administratören aktivt måste välja bort uppdatering av dessa för att gruppförskrivarkoder ska ligga kvar oförändrade. För mer information om hur detta går till, se instruktioner i [Handbok för HSA-administratörer](#).

² Kräver att organisationen i sin HPT gett Inera AB sitt godkännande att hämta dessa uppgifter från Socialstyrelsens register.



9. Checklista för anslutning till Pascal

Syftet med denna checklista är att ge de införandeansvariga i region, kommun och privata vårdgivare en snabbkontroll att organisationen har utfört de aktiviteter som måste genomföras för att få tillgång till Pascal.

- Ansluten till HSA
- Ansluten till SITHS
- SITHS-kort och kortläsare beställda
- Systemkrav och rekommendationer uppfyllda
 - Krav/rekommendationer på operativsystem och webbläsare uppfyllda
 - Krav/rekommendationer på Net iD uppfyllda
 - Brandväggar öppnade
 - Krav/rekommendationer på kortläsare och drivrutin uppfyllda
 - Krav/rekommendation på pdf-läsare uppfyllda
 - Tunna klienter fungerar korrekt (Gäller enbart om man har tunna klienter)
- Datorkrav och rekommendationer uppfyllda
- Användare har erhållit SITHS-kort
- Funktionstest av SITHS/kortläsare utförd
- Lokal support etablerad
- Användare registrerad i HSA
 - Vårdgivare, vårdenhet och verksamhetschef registrerad
 - Registrerat organisationsnummer för aktuell vårdgivare
 - Registrerad postadress och postnummer där verksamheten bedrivs för aktuell vårdenhet
 - Registrerat telefonnummer för aktuell vårdenhet
 - Registrerad arbetsplatskod för aktuell vårdenhet och/eller kopplade enheter
 - Medarbetaruppdrag definierade



- Användare registrerade
- Användare kopplad till medarbetaruppdrag
- Legitimerade yrkesgrupper angivna
- Befattningar angivna (**ej krav**)
- Förskrivarkoder/gruppförskrivarkoder angivna
- Kontroll av HSA-information