

Beslutad av: Vårdens digitalisering, enhet e-tjänster 2020-03-16

Diarienummer: RS-2020 02026-4

Giltighet: från 2022-02-02 tills vidare

Ersätter: RS-2020 02026-1

Rutin

Inloggning och identifiering vid digitala vårdmöten

Rutinen gäller för: Västra Götalandsregionen

Innehållsansvar: Koncernstab digitalisering

Innehåll

Sammanfattning	3
Krav för inloggning och identifiering av mötesdeltagare	3
Val av metod i systemet	4
Alternativ metod för identifiering	4
Inloggning via SMS	4
Inloggning via engångslänk	4
Mötesdeltagare med skyddade personuppgifter.....	5
Identifiering.....	5
Tillgång till personuppgifter i plattformen.....	6
När vårdgivare bjuder in patient till digitalt möte.....	6
När patienten bokar in sig själv till ett digitalt möte.....	6
Flerpartssamtal för patienter med skyddade personuppgifter	6
Inbjudan till andra plattformar	7
Inloggning för vårdutövare	7
Vårdpersonal som deltagare i möte.....	7
Studenter och vikarierande eller annan tillfällig personal	7

Sammanfattning

Dokumentet är avsett för Västra Götalandsregionens digitala mottagningar och är en anvisning för inloggning och identifiering av invånare/patienter, närstående och externa deltagare för deltagande i ett digitalt vårdmöte via Visiba Cares plattform.

Denna rutin beskriver hur verksamheten kan försäkra sig att de har rätt patient som deltagare vid användning av alternativa inloggningar i de e-tjänster som är baserade på Visiba Cares plattform:

- Mitt vårdmöte
- Närhälsan Online
- Ungdomsmottagningen Online
- Folktandvården
- Företagshälsovården

Ett digitalt vårdmöte ska kunna genomföras med en tillfredsställande identifiering av de deltagande parterna.

Krav för inloggning och identifiering av mötesdeltagare

Med *mötesdeltagare* avses här de personer som deltar i ett digitalt vårdmöte, utöver den vårdutövare som är värd för mötet.

För åtkomst till ett digitalt vårdmöte krävs att detta föregås av stark autentisering. Detta innebär att kontroll av uppgiven identitet sker med två olika faktorer, så kallad flerfaktorsautentisering.

Godkända e-legitimationer med stark autentisering är

- **BankID** (BankID är en elektronisk ID-handling som är jämförbar med pass, körkort och andra fysiska legitimationshandlingar).
- **SITHS** (Identifieringstjänst SITHS är en säkerhetslösning och e-legitimation som gör det möjligt för användare att identifiera sig, i tjänsten, med stark autentisering vid inloggning i e-tjänster. Alla regioner, kommuner, privata vårdgivare och statliga myndigheter kan använda Identifieringstjänst SITHS.) SITHS e-ID är godkänd av DIGG (Myndigheten för digital förvaltning).
- e-legitimationer utfärdade av DIGG, så kallade eID:n, samt inom EU eIDAS, ska användas för en säker inloggning och identifiering av invånare/patienter, närstående och vissa externa deltagare som till exempel arbetsgivare för deltagande i ett digitalt vårdmöte.

Val av metod i systemet

Vid inbjudningsfunktionen i systemet så anger vårdpersonal vilken metod för inloggning som ska användas av deltagaren. Om inget val görs av annan metod, används BankID/eID som standard.

Annan metod för inloggning kräver därför att man som vårdpersonal aktivt väljer detta. De metoder som idag erbjuds för deltagarna är att logga in via BankID, SMS eller en möteslänk som automatiskt skickas från systemet via e-post till angiven e-postadress.

Manual/lathund för handhavande i systemet ingår ej i detta dokument.

Alternativ metod för identifiering

Om godkänd e-legitimation inte är tillgänglig, kan vårdpersonal på aktuell mottagning ge tillåtelse att använda annan metod. Tillåtelsen kan endast ges till specifika invånare/patienter för det enskilda tillfället, inte generellt.

Det är ansvarig vårdutövare som ansvarar för att det är rätt personer som deltar i mötet.

Vårdpersonal som bjuds in till ett digitalt vårdmöte **som mötesdeltagare**, kan i vissa fall också ges tillåtelse att använda annan metod för identifiering.

Inloggning via SMS

Vid inbjudning från systemet kan vårdutövaren välja autentiseringsmetod för deltagare. Väljs SMS så måste vårdutövaren ange deltagarens mobilnummer. Vid inloggning till tjänsten får deltagaren sedan möjlighet att välja inloggningsmetod. Hen väljer då SMS-inloggning och får därefter ange sitt mobilnummer för att erhålla en engångskod till mötet. Mobilnumret måste vara samma som vårdutövaren angav vid bokningen av mötet, för att en engångskod ska skickas ut.

Detta får användas av inbjudande mottagning utifrån deras bedömning av enskild patients behov och möjligheter, när patient av olika orsaker inte kan använda BankID eller övriga eID för inloggning.

Bedömning av behov och möjlighet för identifiering via sms görs av inbjudande mottagnings personal utifrån patientens behov och förutsättningar så som ålder, ombud, eventuell funktionsnedsättning, sociala förutsättningar, socioekonomiska förutsättningar med mera. Det är verksamheten som äger kriterierna för bedömningen och hur bedömningen ska genomföras praktiskt.

Inloggning via engångslänk

Detta får användas av inbjudande mottagning för kontakt med en professionell extern deltagare från exempelvis myndigheter, kommuner eller tolkar för deltagande i ett digitalt vårdmöte med patient.

Med professionell avses person som i egenskap av sin yrkesroll innehar ett skäl för att delta i ett digitalt vårdmöte med patient och vårdpersonal.

För användande gäller att inbjudan med engångslänk ska skickas till deltagarens e-postadress som används i tjänsteutövning alternativt funktionsbrevlåda som tillhandahålls av dennes arbetsplats.

Inloggning och autentisering sker då som vanligt i deltagarens arbetsplatsdator för att få tillgång till inbjudan för mötet. Inbjudande mottagning ska vid tveksamheter alltid be deltagaren att uppvisa sin tjänstelegitimation eller dylikt under mötets början.

Mötesdeltagare med skyddade personuppgifter

Hantering av skyddade personuppgifter utgår från VGR:s övergripande riktlinje för detta. Denna riktlinje hittar du här: [Hantering när person har skyddade personuppgifter från Skatteverket](#).

För att skydda den enskilde patientens information behöver särskilda hänsyn tas vid inbjudan, men även då patienten själv bokar in sig till ett digitalt vårdmöte kan speciella instruktioner behövas. Dessa hänsyn och instruktioner beskrivs här.

Som nämnts ovan, ska patienter i utgångsläget identifiera sig med hjälp av en e-legitimation. Detta gäller även för personer med skyddade personuppgifter.

Identifiering

En patients personnummer är centralt för att kunna identifiera personen och därmed säkerställa att vårdutövaren har rätt information angående patienten tillgänglig. Personnumret måste därför alltid vara tillgängligt och synligt för vårdgivaren. Övriga uppgifter relaterat till en patient, som till exempel namn, adress eller telefonnummer, kan ses som känslig information för någon som har skyddade personuppgifter. Dessa bör därför döljas i systemet och inte visas varken för vårdutövaren eller någon annan.

Eftersom detta inte görs med automatik i systemet, behövs viss manuell hantering för att dölja denna information. Aktuella uppgifter i VGR:s plattform för digitala vårdmöten är namn, telefonnummer och e-postadress. Dessa bör alltså inte anges i klartext, utan i förekommande fall ersättas med alternativa tecken, fingerade uppgifter eller utelämnas helt. Det är viktigt att känna till att uppgifterna kan ändras av både vårdpersonal (rollerna *vårdutövare* och *schemaläggare*) och patienten själv. Patienten bör informeras om att hen kan utelämna sitt riktiga namn vid behov.

Exempel: Namn kan anges med ”*****” i respektive namnfält. Fältet för e-postadress kan lämnas tomt.

Angående telefonnummer, så kan en patient i nuläget inte registrera sig som användare i appen utan att ange ett mobilnummer. Att mobilnummer är en obligatorisk uppgift motiveras utifrån att det i normalfallet är nödvändigt att ha tillgång till patientens telefonnummer, dels för att kunna skicka påminnelser i form av SMS, dels för att ha en alternativ kontaktväg i det fall tekniska problem uppstår.

Tillgång till personuppgifter i plattformen

Utöver användare med rollen *Global administratör*, har rollerna *vårdutövare* och *schemaläggare* tillgång till personuppgifter i plattformen. Personuppgifter användaren har tillgång till begränsas till de patienter som finns registrerade i plattformen och är också avgränsat mellan de olika e-tjänsterna.

När vårdgivare bjuder in patient till digitalt möte

Som standard ska alltså även patienter med skyddade personuppgifter bjudas in med angivet personnummer och BankID som identifieringsmetod. Dock ska övriga uppgifter som namn etcetera maskeras enligt ovan.

I de fall patienten inte har möjlighet att använda BankID, kan någon av de alternativa metoderna för identifiering användas. Detta får dock endast göras om vårdgivaren och patienten har en tidigare etablerad kontakt och efter att ha **rådgjort med patienten** om vilken metod som är möjlig att använda med hänsyn till risk för röjande av personuppgifter.

En individuell riskbedömning ska alltid göras med hänsyn till den enskilde patienten, anonym e-post och telefonnummer som inte kan knytas till patient är att föredra.

När patienten bokar in sig själv till ett digitalt möte

Vid tidpunkten för utfärdande av denna riktlinje gäller att en patient som vill boka in sig själv på ett en tid för ett digitalt vårdmöte måste använda sig av BankID som metod för identifiering. Då mobiltelefonnummer är en obligatorisk uppgift att ange för patienten vid registrering i appen, måste också detta anges. Detta mobilnummer används för att skicka en verifieringskod, vilken patienten måste ange som en del av registreringsprocessen. Patienten kan dock ange ”****” i fältet för namn, eller ange ett fingerat namn.

Flerpartssamtal för patienter med skyddade personuppgifter

Flerpartssamtal är av säkerhetsskäl inte tillåtna att genomföras via Visiba Cares plattform, för deltagare som har skyddade personuppgifter. I de situationer där ett flerpartssamtal är nödvändigt att genomföra, hänvisas i stället till någon av de andra plattformar VGR har godkänt för möten med känslig information. Se nedan för mer information.

Inbjudan till andra plattformar

I vissa situationer kan det vara befogat att använda andra plattformar än Visiba Care. Begränsningar i funktionaliteten som till exempel antalet deltagare i flerpartssamtal eller möjlighet till att dela in deltagarna i mindre grupper kan göra att andra plattformar behöver användas.

[På VGR:s intranät finns en vägledning över vilka plattformar som finns tillgängliga för digitala vårdmöten, samt information om hur de kan användas.](#)

I de fall andra plattformar används, där inloggning och identifiering inte finns inbyggt, måste inbjudan till mötet skickas på ett sådant sätt att det endast är den avsedda mottagaren som kan ta del av inbjudan. Exempel på detta kan vara att skicka inbjudan via meddelandefunktionen i e-tjänsterna på 1177. Om det finns en tidigare etablerad kontakt via till exempel Mitt vårdmöte, Närhälsan Online eller någon av de andra tjänsterna, kan inbjudan förmedlas via den plattformen.

Det är viktigt att i dessa fall informera mötesdeltagaren om vilken plattform som kommer att användas för mötet och hur anslutning till mötet sker.

Inloggning för vårdutövare

Vårdpersonal som loggar in i plattformen med någon av rollerna *vårdutövare*, *administratör* eller *schemaläggare* ska i normalfallet använda sig av SITHS som metod för identifiering. Verksamhetschef kan i särskilda fall godkänna inloggning med BankID som metod för identifiering.

Vårdpersonal som deltagare i möte

Vårdpersonal som bjuds in som deltagare i ett digitalt vårdmöte och som finns upplagda som användare i plattformen, ska bjudas in som *Kollega* och logga in med SITHS som metod för identifiering.

Bjuds vårdpersonal in som deltagare med rollen *Gäst*, kan metod för identifiering väljas av den som bjuder in till mötet. I första hand bör då SITHS väljas som metod. Om vårdpersonalen i det aktuella fallet inte har möjlighet att identifiera sig med SITHS, kan någon av de andra metoderna väljas.

Studenter och vikarierande eller annan tillfällig personal

Studenter eller annan tillfällig personal som ska genomföra digitala vårdmöten som vårdutövare bör tilldelas en användarlicens och logga in med SITHS som metod för identifiering. Användarlicensen kan sedan tas bort när behovet av den inte längre finns kvar.

I de fall personen inte har en SITHS-legitimation utfärdad, bör användaren i systemet kompletteras med personnummer och BankID användas för identifiering.

Studenter som deltar i ett digitalt vårdmöte i utbildnings- eller studiesyfte, kan bjudas in med någon av ovanstående metoder för identifiering vid inloggning.