



Digitalisering och IT

Systemförvaltningsgrupp ÖNH & Audiologi

ANVISNING

Process 2.1.5 Utöva tillsyn
Skapad av Mie Claesson Magnell
Godkänd av Staffan Strömblad

Godkänt datum 2025-01-22
Version 1.0
Ärendenummer

Loggutdrag Auditbase

Innehåll

Loggutdrag Auditbase.....	1
1 Behörigheter	3
2 Genomförande tillvägagångssätt.....	3
2.1 Att tänka på vid granskning av loggutdrag	3
2.2 Stickprovskontroll	3
2.2.1 Urval.....	3
2.2.2 Tillvägagångssätt	4
2.3 Riktad kontroll	5
2.3.1 Urval.....	5
2.3.2 Tillvägagångssätt	5
3. Dokumentera och rapportera	7
4. Vid misstanke om dataintrång	7

1 Behörigheter

Om verksamhetschefen väljer att delegera handläggning av loggkontroll ska delegeringen vara skriftlig.

För att utföra loggkontroll måste behörighet till Auditdata - Auditbase administration finnas. Det beställs av verksamhetschef via e-post till mottagningens verksamhetsansvarig/verksamhetsspecialist Auditbase, som lägger behörighet.

2 Genomförande tillvägagångssätt

2.1 Att tänka på vid granskning av loggutdrag

- Tidpunkt. Är användaren inne i journaler på avvikande klockslag?
- Förekommer mycket aktivitet i journaler där läsning är av större intresse?
- Förekommer läsning av journal där användaren har känt släktskap eller samma efternamn som patienten?
- Förekommer läsning av kollegas audiogram?
- Förekommer läsning av journal på patient med skyddade personuppgifter?
- Förekommer läsning av journal där patient har medialt intresse?
- Förekommer läsning av journal där patient som av någon anledning väcker annan uppmärksamhet?
- Förekommer läsning av egen journal?

2.2 Stickprovskontroll

2.2.1 Urval

Slumpmässigt urval ska göras varje månad med riktmärke 10% av personalen. Även person som utför loggkontroll ska följas upp om det är aktuellt. Personalens aktivitet under 24 timmar ska granskas.

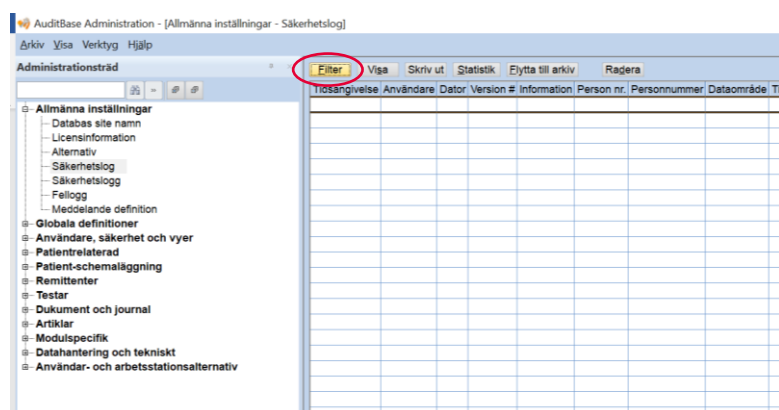
Vid slumpmässigt urval kan slumpgenerator i Excel användas. Det finns en separat guide för hur det fungerar på Vårdgivare i Skåne.

I Auditbase under Användare, säkerhet och vyer, Användaradministration och säkerhet och därefter Anv.rättigheter och inställningar öppnas med +-tecken under respektive vårdenhet uppgift om de användare som är knutna till vårdenheten och som därmed ska granskas.

2.2.2 Tillvägagångssätt

Behörig loggkontrollant loggar in på Auditdata, Auditbase Administration med användarnamn och lösenord.

Under Allmänna inställningar välj Säkerhetslog och därefter Filter



Välj mellan vilka datum och eventuella tider som aktivitet ska granskas.

Välj Signatur på person som ska granskas genom att söka fram för- och efternamn i rullist. Markera signaturen.

Tryck OK

Säkerhetslogfilter

Datum/idsintervall

Från 2024-10-04

Till 2024-10-04

Personnummer:

Person nr.

Daturnamn:

Tabell:

Signatur:

Tilläggstext:

Action

- Admin setup
- Användare beviljats kontakt
- Användare skapad
- Användarerättigheter beviljade
- Användarerättigheter beviljade
- Användarerättigheter upphävida
- Användarkonto raderad
- BrevDokument/Bilagor sända via e-post
- Elektronisk inlämning
- E-post adress uppdaterad
- Fullständig klientdata utskrivnen/exporterad
- Global patient avmarkerad
- Global patient ändrad
- Inloggad

För åtgärden "Admininställning" välj ett "Ytterligare text"-objekt från listan. För "Admininställning " eller andra åtgärder skriv en Ytterligare text att filtrera.

Ok Avbryt

Lista med resultat visas. Resultat ska granskas och värderas.

Filter	Visa	Skriv ut	Statistik	Flytta till arkiv	Radera				
Tidsangivelse	Användare	Dator	Version #	Information	Person nr.	Personnummer	Detaljer	Tilläggstext	
2023-05-15 13:58:51:543000	A110835	RS30139473	5.4.5 9591	Läser av Audiogram daterad 2023-04-12	AudNumber: 4	121212121212	73435	Audiogram	AudNumber: 4
2023-05-15 13:58:35:996000	A110835	RS30139473	5.4.5 9591	Läser av Patient PCODE: 121212121212		121212121212	73435	Patient	PCODE: 121212121212

2.3 Riktad kontroll

2.3.1 Urval

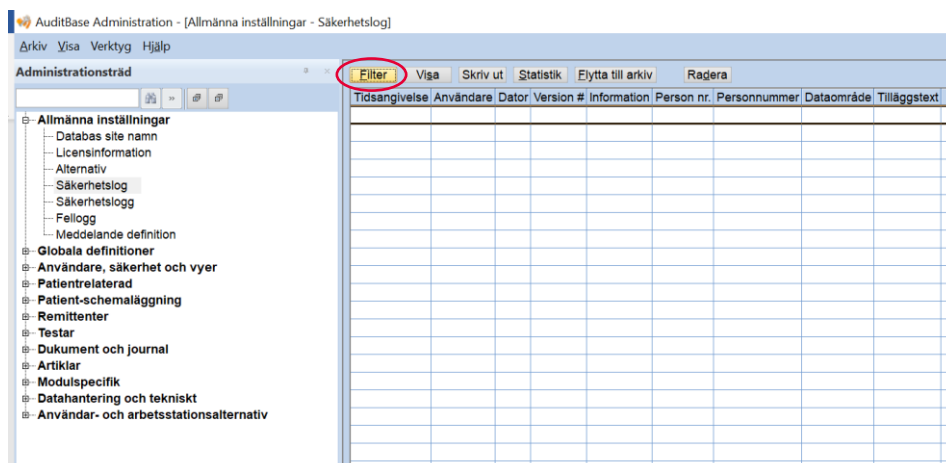
Riktad kontroll ska göras både utifrån personals och patients identitet och ska göras vid de tillfällen då någon av följande företeelser inträffar:

- Misstanke om obehörig åtkomst. Valda patienter.
- Vid vård av patient med skyddade personuppgifter.
- Vid forcering av spärr, oavsett om forcering skett med samtycke eller Nödöppning.

2.3.2 Tillvägagångssätt

Behörig loggkontrollant loggar in på Auditdata, Auditbase Administration med användarnamn och lösenord.

Under Allmänna inställningar välj Säkerhetslog och därefter Filter



Fyll i mellan vilka datum och eventuella tider granskningen gäller.

Fyll i personnummer på den patient vars uppgifter ska granskas.

Tryck OK.

Datum/tidsintervall
Från 2024-04-15
Till 2024-04-15

Personnummer
Person nr. 19121212-1212

Daturnamn
Tabell
Signatur
Tilläggsstext

Action
Admin setup
Användare beviljats kontakt
Användare skapad
Användarerättigheter beviljade
Användarerättigheter beviljade
Användarerättigheter upphävd
Användarkonto raderad
Brev/Dokument/Bilagor sända via e-post
Elektronisk inlämning
E-post adress uppdaterad
Fullständig klientdata utskrivnen/exporterad
Global patient avmarkerad
Global patient ändrad
Inloggad

För åtgärden "Admininställning" välj ett "Ytterligare text"-objekt från listan. För "Admininställning" eller andra åtgärder skriv en Ytterligare text att filtrera.

OK Avbryt

Logglista visas. Resultat granskas och värderas. Här framkommer till exempel tiden då personuppgiften och audiogrammet öppnades och stängdes, vem som öppnat, från vilken dator med mera.

Tidsangivelse	Användare	Dator	Version #	Information	Person nr.	Personnummer	Dataområde
2023-05-15 13:59:17.699000	A110835	RS30139473	5.4.5.9591	Global patient avmarkerad	121212121212	73435	Global patient av
2023-05-15 13:58:51.543000	A110835	RS30139473	5.4.5.9591	Läser av Audiogram daterad 2023-04-12 AudNumber: 4	121212121212	73435	Audiogram
2023-05-15 13:58:35.996000	A110835	RS30139473	5.4.5.9591	Läser av Patient PCODE: 121212121212	121212121212	73435	Patient
2023-05-15 13:58:35.965000	A110835	RS30139473	5.4.5.9591	Global patient ändrad	121212121212	73435	

3. Dokumentera och rapportera

Resultat av utförd loggkontroll ska rapporteras på avsedd sida. Stickprovskontroll och olika riktade kontroller rapporteras var för sig. Genom dessa rapporter får bland annat verksamhetschef information om att loggkontroll utförts. Rapporterade uppgifter används för statistik och uppföljning.

[Registrering och sammanställning av loggkontroller - Region Skånes intranät \(skane.se\)](#).

4. Vid misstanke om dataintrång

Kontakta omgående den verksamhetschef som delegerat uppdraget vid misstanke om dataintrång. Verksamhetschefen ansvarar för att eventuell misstanke om dataintrång utreds och hanteras enligt instruktion *Dataintrång – åtgärder om olovlig åtkomst*.

[Registrering och sammanställning av loggkontroller - Region Skånes intranät \(skane.se\)](#)