

Informationssäkerhetspolicy för elevhälsans medicinska insats – AcadeMedias gymnasiesegment

Dokumentägare: Medicinsk verksamhetschef AcadeMedias gymnasiesegment

I AcadeMedias gymnasiesegment ingår ett antal enskilda bolag. Varje enskilt bolag är juridiskt sett en enskild vårdgivare. Inom AcadeMedia, liksom i denna policy, används begreppet verksamhet, ett begrepp som avser varje enskilt bolag.

Elevhälsans medicinska insats (EMI) utgörs av befattningarna skolsköterska och skolläkare. För EMI har respektive vårdgivare en utsedd verksamhetschef i enlighet med 29 § Hälso- och sjukvårdslagen (1982:763). Denna funktion benämns inom AcadeMedias gymnasiesegment för medicinsk verksamhetschef (MVC).

Funktion MVC har det operativa ansvaret för att det systematiskt bedrivs ett kvalitets- och patientsäkerhetsarbete. Uppdragets innebörd och omfattning finns dokumenterat i en delegationsordning från vårdgivarna till utsedda för uppdraget.

Informationssäkerhetsarbete inom AcadeMedias gymnasiesegment

Denna informationssäkerhetspolicy omfattar alla verksamheter inom AcadeMedias gymnasiesegment och syftar till att uppfylla kraven i patientdatalagen (2008:355) samt Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). Denna informationssäkerhetspolicy är en del av vårdgivarnas ledningssystem för kvalitet och patientsäkerhet. Ledningssystemet i sin helhet ger svar på hur vårdgivarna arbetar med områdena tillgänglighet, riktighet, sekretess och spårbarhet. Se nedan för innebörden av respektive område.

- Patientuppgifter i vårdgivarens dokumentation är åtkomliga och användbara för den som är behörig (tillgänglighet).
- Patientuppgifterna är oförvanskade (riktighet).
- Obehöriga ska inte kunna ta del av patientuppgifterna (sekretess).
- Det är möjligt att i efterhand entydigt kunna härleda åtgärder till en identifierad användare (spårbarhet).

Ansvarsfördelning – medicinsk verksamhetschef

- Inom ramen för Informationssäkerhetsarbetet ansvarar MVC för att:
- Patientuppgifternas kvalitet och ändamålsenlighet följs upp.



Academedias

- Utdelningen av behörigheter för åtkomst till patientuppgifter är ändamålsenliga och förenliga med skolsköterskornas och skolläkarnas aktuella arbetsuppgifter.
- Skolsköterskorna och skolläkarna är informerade om de bestämmelser som gäller för hantering av patientuppgifter och att det finns rutiner för hur dokumentationen ska genomföras.
- Följa upp informationssystemens användning genom att tillse att det regelbundet sker kontroll av användarnas loggar.

I enlighet med gällande föreskrift åligger det MVC att minst en gång per år rapportera till vårdgivarna om informationssäkerhetsarbetet. Rapporten ska innehålla uppgifter om granskningar och skyddsåtgärder av större betydelse som gjorts i enlighet med informationssäkerhetspolicyn, riskanalyser som utförts av informationssäkerheten och förbättringsåtgärder som vidtagits. Inom AcadeMedias gymnasiesegment ska denna återkoppling ske skriftligen under juni månad.

Ansvarsfördelning – skolsköterska/skolläkare

Skolsköterskorna och skolläkarna ska:

- Ansvara för att personliga lösenord och hjälpmedel för autentisering inte är eller kan bli tillgängliga för obehöriga.
- Ansvara för att datorer eller andra informationsbärare som har använts inte lämnas utan att patientuppgifterna är skyddade från obehörig åtkomst.
- Endast ta del av patientuppgifter där hen deltar i vården av eleven/patienten eller för något annat ändamål som anges i 2 kap. 4 och 5 § patientdatalagen (2008:355) behöver uppgifterna för sitt arbete inom Elevhälsans medicinska insats.
- Signera sin dokumentation.
- Se till att patientjournalen är försedd med en entydig personidentifikation.
- Se till att patientjournalen är försedd med elevens/patientens senast kända adress eller att andra kontaktuppgifter är angivna.
- Följa vårdgivarnas rutiner för dokumentation.
- Följa vårdgivarnas rutiner för hur journaler ska hanteras.

Profdoc Medical Office (PMO)

EMI använder PMO, vilket är ett elektroniskt journalsystem som stödjer hanteringen av medicinsk dokumentation och patientadministration. PMO är CE-certifierat som en medicinteknisk produkt. Verksamheterna har inte sammanhållen journalföring med varandra eller någon annan part. Ingen patient/elev eller vårdnadshavare har enskild direktåtkomst till sina patientuppgifter eller sitt barns patientuppgifter.

För PMO finns det alltid en generell säkerhetskopia som finns kvar i 30 dagar. Det tas dagligen en säkerhetskopia där enbart ändringar sedan den senaste säkerhetskopian tas med. Varje helg görs sedan en fullständig säkerhetskopiering. Säkerhetskopian skapas och förvaras på annan plats än originalet. Återläsningstest görs en gång per år och resultatet av det redovisas i samband med att MVC återrapporterar om informationssäkerhetsarbetet till vårdgivarna.



Tillgänglighet, riktighet, sekretess och spårbarhet

Nedan följer en beskrivning för hur vårdgivarna lever upp mot kraven relaterat till områden tillgänglighet, riktighet, sekretess och spårbarhet.

Tillgänglighet

AcadeMedia driftar PMO. För att säkerställa drift och förvaltning finns en utsedd systemägare och en förvaltningsorganisation enligt PM3. Planerade driftstopp görs i samförstånd mellan IT och verksamheterna. Oförutsedda driftstopp hanteras i enlighet med AcadeMedias eskaleringsrutiner för verksamhetskritiska system.

Behörig användare loggar in mot en domän för att sedan via fjärrskrivbord kunna komma åt PMO. För att säkerställa stark autentisering för åtkomst används SITHS-kort vid inloggning till PMO. Användning av PMO-Client ska ske på arbetsplatsen av behörig användare. Undantag kan beviljas av MVC. Användning av PMO-admin bör ske från arbetsplatsen av behörig användare.

Innan anställning eller konsultuppdrag påbörjas kontrolleras skolsköterskans/skolläkarens hsa-Id och legitimation. När en behörig användare avslutar sin anställning eller konsultuppdrag inaktiveras användaren i PMO och därigenom spärras åtkomsten till patientuppgifter.

Sekretess

MVC ansvarar för att behöriga befattningshavares åtkomst begränsas till vad som är nödvändigt för att kunna ge god och säker vård. Vårdgivarna har enats om använda de tre behörighetsnivåerna administratör, skolsköterska/skolläkare samt It-tekniker. Administratörsnivån ger behörighet till att utföra administrativa uppgifter i Admin-client. Exempel på administrativa uppgifter är att lägga till nya användare, inaktivera användare och arkivera journaler. Behörighetsnivå skolsköterska/skolläkare ger åtkomst till patientuppgifter. Behörighetsnivån It-tekniker ger endast åtkomst till en fiktiv skola och fiktiva patienter.

När en behörig användare ska ta fram patientuppgifter ska det ske genom att söka patient/elev på fullständigt personnummer eller via en sökfunktion som per automatik endast ger aktuella patienter/elever på aktuell skola sökbara. Om behörig användare inte uppger korrekt personnummer för aktuell patient/elev och får fram en annan av vårdgivarens patienter/elever kan användare inte öppna journalen utan att göra ett aktivt val samt skriva en kommentar till det aktiva valet. Detsamma gäller om patientuppgifterna har spärrats av en annan vårdenhet hos vårdgivaren, då kan uppgifterna endast göras tillgängliga efter det att den behörige användaren gjort ett aktivt val efter ett inhämtat samtycke eller om förutsättningarna för nödåtkomst enligt 4 kap. 5 § patientdatalagen (2008:355) är uppfyllda.

Riktighet

I PMO framgår det vem som svarar för en viss journaluppgift, dennes befattning samt tidpunkt för när journaluppgiften fördes in i patientjournalen. Dokumenterade journaluppgifter kan inte ändras eller utplånas av behöriga användare. Införda uppgifter ska signeras i samband med att de dokumenteras.

Varje enskild patientjournal förses med entydig personidentifikation samt med eleven/patients senaste kända adress eller andra kontaktuppgifter.

Elever/patienter med skyddad personuppgifter ska inte finnas i PMO. Pappersjournal ska upprättas för denna grupp i enlighet med vårdgivarnas rutiner.



AcadMedia

Spårbarhet

I PMO loggas användarnas aktiviteter. Det går att se vilken användare och från vilken enhet en elevs/patients journal har öppnats. Vidare går det att se vilka åtgärder som vidtagits med patientuppgifterna. Det genomförs systematiska och återkommande loggar på alla användare. Genomförda kontroller och loggar sparas i minst 10 år.

