Risikovurdering for brug af Noteless i Min Sundhedsklinik - (Sololægeklinik)

Dataansvarlig og bruger af noteless: Læge Mobarak Shah Atef

Godkendt dato: 25.05.2026

Formål og afgrænsning

Denne risikovurdering er udarbejdet af og for Min Sundhedsklinik som dataansvarlig og omfatter udelukkende klinikkens egen brug af Noteless som transskriptions- og dokumentationsværktøj. Vurderingen er ikke en generel vurdering for andre klinikker eller for sundhedsvæsenet som helhed.

Formålet er at dokumentere, at den konkrete brug af Noteless i Min Sundhedsklinik kan ske på en måde, der er forenelig med GDPR, reglerne for behandling af helbredsoplysninger og Datatilsynets forventninger til brug af AI og talegenkendelse i sundhedsvæsenet.

Kort beskrivelse af Noteless og behandlingen

Noteless er en skybaseret software-as-a-service (SaaS) platform, der i realtid omdanner samtalen mellem læge og patient til tekst og udkast til journalnotater og dokumenter. I klinikkens brug forstås dette som live-transskription: lydsignalet sendes i realtid til transskription og lagres ikke som en lydfil, der kan afspilles i Noteless. Tjenesten fungerer som dokumentationshjælpemiddel, ikke som journalsystem eller selvstændig klinisk beslutningsstøtte.

Ifølge databehandleraftalen transskriberer Noteless lyd til tekst, anonymiserer direkte identifikatorer (bl.a. personnummer og telefonnummer) før videre AI-behandling og omdanner teksten til et struktureret notatudkast, som kan kopieres til klinikkens journalsystem. Genererede noter og transskriptioner slettes automatisk senest 24 timer efter konsultationen.

De oplysninger, der behandles, er helbredsoplysninger om patienter og eventuelle tredjepersoner, som omtales under konsultationen, herunder kliniske vurderinger, symptomer, undersøgelser og behandlingsplaner.

Roller og retsligt grundlag

Min Sundhedsklinik er dataansvarlig (controller) for den behandling af personoplysninger, der sker i forbindelse med brug af Noteless, mens Noteless er databehandler (processor) i henhold til GDPR-artikel 28 (krav til databehandleraftaler og passende garantier, når behandling sker på vegne af den

dataansvarlige). Databehandleraftalen fastlægger, at Noteless kun må behandle personoplysninger efter dokumenterede instrukser fra klinikken og alene til at levere og forbedre den aftalte tjeneste.

Der behandles særlige kategorier af personoplysninger i form af helbredsoplysninger, som er omfattet af de skærpede regler i GDPR-artikel 9 (særlige kategorier af oplysninger, herunder helbredsoplysninger) og Datatilsynets vejledning om helbredsoplysninger. Retsgrundlaget er kombinationen af sundhedslovgivningens journal- og dokumentationspligt og GDPR-artikel 9, stk. 2, litra h (behandling nødvendig med henblik på forebyggende sundhed, medicinsk diagnostik og behandling m.v. udført af sundhedspersoner), samt relevant national regulering om behandling af helbredsoplysninger i sundhedsvæsenet.

Sikkerhedsforanstaltninger hos Noteless

Databehandleraftalen og sikkerhedsbilag beskriver, at Noteless anvender kryptering ved overførsel og lagring af kundedata, adgangsstyring, logning, adskillelse af kunders data og regelmæssige interne sikkerhedsaudits. Patienttransskriptioner, noter og relaterede konsultationsdata slettes automatisk inden for 24 timer som led i systemets standarddesign.

Der er krav om multifaktor-autentifikation, begrænsning af privilegerede adgange, omfattende logning og overvågning samt passende beskyttelse mod digitale angreb. Kundedata må ikke bruges til test uden særskilt skriftlig aftale, og der er etableret procedurer for komplet sletning eller returnering af data, herunder backup og logfiler, ved ophør eller efter instrukser fra den dataansvarlige.

Databehandleraftalen fastslår desuden, at eventuelle overførsler til tredjelande kun må ske efter klinikkens dokumenterede instrukser eller til tredjelande med gyldigt overførselsgrundlag (fx EU-tilstrækkelighedsafgørelse) i overensstemmelse med GDPR-kapitel V. En opdateret liste over underdatabehandlere er tilgængelig i Noteless' Trust Center, hvor klinikken kan holde sig orienteret og gøre indsigelse.

Klinikkens konkrete brug og lokale kontroller

I Min Sundhedsklinik anvendes Noteless efter følgende grundprincipper:

- Noteless kører som et separat program på en klinik-pc og har ingen teknisk integration eller direkte adgang til det anvendte journalsystem.
- Noteless bruges alene til live-transskription af samtalen og til at generere udkast til notater og attester; det endelige journalnotat oprettes og gemmes udelukkende i klinikkens autoriserede journalsystem.

- Efter journalnotatet er oprettet i klinikkens journalsystem, slettes udkastet i Noteless som led i klinikkens rutine; eventuelle resterende udkast, der ikke er slettet manuelt, slettes automatisk af Noteless senest 24 timer efter konsultationen.
- Lægen gennemgår altid udkastet, retter og supplerer efter faglig vurdering, før notatet kopieres ind i journalen.
- Som fast arbejdsgang i soloklinikken undlader lægen så vidt muligt at indtale eller indtaste CPR-numre, fulde navne, adresser og andre unødvendige direkte identifikatorer i Noteless, ud over hvad der er strengt nødvendigt for den konkrete dokumentation.
- Noteless-kontoen er personlig, beskyttet med stærk autentifikation (MitID) og anvendes udelukkende af klinikkens læge/ejer.
- Klinikkens generelle it-sikkerhedsforanstaltninger (opdaterede systemer, skærmlås, fysisk sikring af lokaler m.v.) gælder også for den pc, hvor Noteless anvendes.
- Der er procedurer for at sikre, at live-transskriptionen stoppes ved konsultationens afslutning, så utilsigtet behandling af næste patients samtale undgås.
- Ved dagens afslutning lukkes Noteless-programmet som led i klinikkens rutine, så der ikke står aktive udkast åbne på skærmen.
- Patienter informeres om brugen af Noteless via klinikkens hjemmeside samt via opslag og informationsfoldere i reception og konsultationsrum, herunder om formålet med live-transskription, sletning inden for 24 timer og muligheden for at sige nej til brugen.
- Der foreligger en intern procedure for håndtering af eventuelle databrud, herunder vurdering, anmeldelse til Datatilsynet og information til de berørte patienter i overensstemmelse med GDPR.

Patientinformation og transparens

Noteless' privatlivspolitik beskriver overordnet, hvordan personoplysninger, herunder helbredsoplysninger, behandles og beskyttes. Min Sundhedsklinik supplerer dette med lokal information til patienterne via opslag og informationsfolder i receptionen og konsultationsrummet om, at et sikkert AI-baseret transskriptionsværktøj kan anvendes under konsultationen.

Det fremgår af informationen, at:

- Samtalen live-transskriberes til tekst for at hjælpe lægen med notatskrivning; samtalen lagres ikke som en lydoptagelse, der kan afspilles i Noteless.
- Transskriptionen kun bruges til at lave notater og eventuelle udkast til attester.

- Noteless ikke har adgang til klinikkens journalsystem.
- Data i Noteless slettes automatisk efter kort tid (max. 24 timer).
- Lægen fortsat har det fulde behandlings- og journalansvar.
- Patienten kan sige fra, hvis vedkommende ikke ønsker, at Noteless anvendes ved særlige konsultationer.

Denne transparens ligger i tråd med Datatilsynets fokus på tydelig information ved brug af AI og behandling af helbredsoplysninger.

CE-mærkning, medicinsk udstyr og ansvar

Noteless' egne vilkår beskriver tjenesten som et dokumentations- og administrativt hjælpeværktøj, der kun skal støtte sundhedspersonens beslutninger; alle udkast skal fagligt gennemgås og kan ikke erstatte klinisk vurdering. Offentligt tilgængelige kilder beskriver, at Noteless har valgt at CE-mærke løsningen som medicinsk udstyr, hvilket indebærer et formelt fokus på risikostyring og kvalitet, men ændrer ikke ved, at det endelige behandlingsansvar fortsat ligger hos klinikkens læge.

I Min Sundhedsklinik anvendes Noteless konsekvent kun til udkast, og systemet fungerer ikke som system-of-record for patientjournaler; dette reducerer risikoen for, at fejl i transskription eller genererede forslag direkte fører til fejlagtig diagnosticering eller behandling.

Centrale risici

For Min Sundhedsklinik vurderes de væsentligste risici ved brug af Noteless som:

- Risiko for uautoriseret adgang til tekstdata og den underliggende midlertidige behandling af lydsignalet (brud på fortrolighed).
- Risiko for utilsigtet behandling af samtaler med andre personer end den aktuelle patient, hvis live-transskriptionen ikke stoppes korrekt.
- Risiko for fejl i transskription eller AI-genererede udkast, som kan medføre fejl eller udeladelser i journalnotatet.
- Risiko for, at data ikke slettes korrekt efter 24 timer, eller at anonymisering er utilstrækkelig.
- Risiko for problematiske dataoverførsler til tredjelande eller underdatabehandlere uden tilstrækkelige garantier.

En offentliggjort risikovurdering fra en dansk almen praksis, der anvender Noteless på en lignende måde (separat værktøj, automatisk sletning, ingen journalintegration), vurderer disse risici som lav til

moderate, når der er etableret stærk kryptering, tidsbegrænset lagring, klar rollefordeling og manuel faglig gennemgang. Dette understøtter vurderingen i nærværende dokument.

Risikiminimerende foranstaltninger og samlet vurdering

De beskrevne tekniske sikkerhedsforanstaltninger hos Noteless kombineret med Min Sundhedskliniks lokale kontroller reducerer de identificerede risici væsentligt. Særligt vigtigt er, at Noteless kun bruges som dokumentationshjælpemiddel uden journalintegration, at alle notater gennemgås manuelt, og at data kun lagres i kort tid.

På den baggrund vurderes den samlede risiko for patienternes rettigheder og frihedsrettigheder ved den beskrevne brug af Noteless i Min Sundhedsklinik som lav til moderat og acceptabel under følgende forudsætninger:

- Noteless fortsat opfylder de beskrevne sikkerhedskrav, herunder kryptering, adskillelse af data og automatisk sletning inden for 24 timer.
- Klinikken opretholder de lokale kontroller (ingen journalintegration, begrænset brug af identifikatorer, stærk autentifikation, interne instrukser og procedurer for databrud).
- Klinikken løbende holder sig orienteret om Noteless' underdatabehandlere og eventuelle tredjelands-overførsler via Trust Center og reagerer, hvis der opstår tvivl om overensstemmelse med GDPR kapitel V.

Min Sundhedsklinik vil revurdere denne risikovurdering mindst én gang årligt og ved væsentlige ændringer i Noteless' funktionalitet, databehandleraftale, underdatabehandlere eller i de regulatoriske rammer for brug af AI i sundhedsvæsenet.

Bilag (opbevares sammen med denne risikovurdering):

- Databehandleraftale med Noteless.
- Noteless' privatlivspolitik.
- Seneste udskrift/eksport af liste over underdatabehandlere fra trust.noteless.com.