Dokumentnavn	Retningsgivende dokument for personoplysninger og diskretion. Version 2
Dato for ikrafttrædelse	1. oktober 2015 til 30. september 2018
Revideres senest (dato)	30. september 2018
Ansvarlig for dokumentet	Indehaver
Godkendt af	Indehaver
Formål	At sikre • beskyttelse mod misbrug og tab af personoplysninger • patientens diskretion i kontakten med klinikken
Hvem gælder dokumentet for?	Alle ansatte i klinikken
Fremgangsmåde	**Personalets adgang til og omgang med patientoplysninger** • Alle ansatte skal være bekendt med regler for indhentning og håndtering af patientoplysninger - opslag må kun ske med et formål og patientaccept hertil skal sikres • Alle medarbejdere skal have egen log-on kode og eventuel digital signatur • Log on lister skal gemmes digitalt i 6 måneder (system udbyder) • Medarbejderes id, eksamenspapirer etc skal sikres ved ansættelse • Ansatte skal være indforstået med tavshedspligt under og efter ansættelsen **Information, samtykke og videregivelse af patientoplysninger** • Patienten skal give samtykke til behandling forudgået af dialog omkring behandlingen • Patienten skal være fyldt 15 år for at kunne afgive samtykke (hvis en patient på 15-17 år ikke er i stand til at forstå konsekvenserne af sin stillingtagen skal forældremyndigheds-indehaveren give samtykke til behandling) • Er patienten under 15 år skal forældremyndighedsindehaveren give samtykke men patienten skal stadig inddrages i dialogen. • For varigt inhabile patienter skal værge give samtykke (men behandling må ikke gennemføres med tvang hvis patienten i ord eller handling sætter sig til modværge)

- Ved øjeblikkelig behandlingsbehov, hvor patienten ikke kan give samtykke, må behandling institueres (nødbehandling)
- Mundtlig samtykke er nok (fraset sterilisationer hvor skriftlig samtykke også skal foreligge)
- Information til patienten skal være grundig, især hvis der kan være risiko for komplikationer
- Patienten kan frabede sig information (skal i så fald noteres i journalen)
- Patienten skal informeres om at epikrise sendes til henvisende læge (og patienten kan modsætte sig dette)
- Information omkring behandlinger gives altid mundtlig og hvor det skønnes hensigtsmæssigt også skriftligt.
- Samtykke til behandling medfører også samtykke til videregivelse af informationer, parakliniske resultater mm som er en naturlig forlængelse af den initielle behandling (behandling med efterfølgende henvisning til hospitalet). Patienten kan dog frabede sig dette, og skal derfor være oplyst om denne mulighed
- Videregivelse af patientoplysninger til f.eks forsikringsselskaber skal forudgås af skriftlig samtykke/digital signatur fra patienten
- Information og samtykke skal journalføres incl. hvad der er videregivet
- Patienten kan til enhver tid tilbagekalde sit samtykke

Datasikkerhed og sikring af patientfølsomme oplysninger

Ved patientfølsomme oplysninger forstås alle dokumenter som identificerer patienter ved navn, cpr-nummer, billeder eller adresser.

- Klinikken er aflåst, når den ikke er bemandet
- Klinikken har alarm
- Bygningen, hvori klinikken er beliggende, er aflåst og sikret med alarm
- Computer/-e er sikret med adgangskode
- Indehavere af adgangskode til computer/-e er nedskrevet
- Fjernbackup er sikret og krypteret
- Sæt evt. et skilt/dokument op i klinikken, hvorpå der står, hvem der er den dataansvarlige (oftest speciallægen), samt hvem der har adgang (sekretær/sygeplejerske/andre). Her kan også stå omkring videregivelse af personhenførbare data (sygehus, anden speciallæge, forsikring, andre?)
- Data skal som udgangspunkt altid håndteres og opbevares så uvedkommende ikke gives umiddelbar adgang til disse.
- Computer/-e er slukket/skærmen låst/slukket, hvis den/de forlades.

	• Patientfølsomme oplysninger ligger aflåst eller utilgængelig for uvedkommende • Opbevaring i ikke-observerede omgivelser skal ske i aflåste rum, skabe eller arkiver. • Ved hjemmearbejdsplads, hvor klinikkens hovedcomputer tilgås, skal det ske via krypteret adgang • Hjemmecomputeren må ikke kunne åbnes af andre end indehaveren eller associeret godkendt personale • Det elektroniske arkiv er beskyttet af firewall via it-leverandøren og forsendelser sker krypteret på beskyttede netværk. Backup foretages krypteret (sikret med _____) på en ekstern server udenfor klinikken (_____). • Klinikken bør have papirdokumentation på, at udbyder har sikker opbevaring af personhenførbare data • Ved backup i klinikken på extern harddisk, skal denne sikres i aflåst skab eller lignende • Udvekslingen af personoplysninger via Sundhedsdatanettet er automatisk sikret mod uretmæssig adgang og sker ved kryptering, firewall, anti-virusprogram ect. • Personoplysninger må ikke indhentes eller videregives uden patientens accept. Dette gælder dog ikke anmeldelser til nationale registre. Sidstnævnte hvis man bruger diagnosekoder • Personfølsomme oplysninger, der benyttes til egne statistikker og til videnskabeligt formål skal sikres på samme vilkår som al anden data i klinikken. • Patienters stamdata indhentes ved opslag i CPR-registret og henvisning hentes fra RefHost og sammenholdes herefter med oplysningerne på patientens sundhedskort. Andre data indhentes via Sundhed.dk (efter patientsamtykke) og FMK. • Bøger eller lister med fortegnelser over laboratoriedata og lignende, der indeholder patientfølsomme oplysninger, skal opbevares i aflåst arkiv/skab, når de ikke er i brug. Under anvendelse skal bøger og lister placeres så tilfældigt forbipasserende ikke umiddelbart kan tilegne sig oplysninger fra dem. • Alle klinikkens computere skal være beskyttet af personlig log-in. Monitoren skal altid være placeret således, at den ikke kan aflæses af tilfældigt forbipasserende. Afsendelse af persondata må kun ske internt på klinikkens beskyttede net eller via eksterne beskyttede net, og således ikke sendes med almindelig e-mail eller andre åbne medier. • Fax-/kopimaskine: Fax betegnes som et sikkert medie til afsendelse og modtagelse af data, men man skal være fuldt bekendt med modtagerens identitet. Ved egen modtagelse eller efter kopiering skal materialet straks flyttes til den tiltænkte arbejdsplads eller arkiv.

	• Billedmateriale skal håndteres på linje med andre former for patientfølsomme oplysninger. • Dagslister/operationsprogrammer. Disse lister fremstilles fra dag til dag, og skal benyttes og opbevares lige så sikkert som alle andre personfølsomme oplysninger. De skal makuleres efter endt arbejdsdag. • Ved systemfejl skal speciallægen og support afdelingen for it-leverandøren kontaktes. • Bortskaffelse af patientfølsomme oplysninger: Papirmateriale bliver makuleret. Elektroniske data i konsoller eller servere som kasseres, skal slettes ved dobbelt formatering og fysisk ødelæggelse af diskdrevene. **Papir-journaler (i klinikker der ligger inde med dette)** • Generelt forefindes der så lidt papirjournal som muligt, idet der anvendes EPJ og eksterne dokumenter scannes ind. • Papir-journaler opbevares i aflåste arkiver og er dermed sikret mod uvedkommendes adgang. • Der må kun udtages journaler som umiddelbart skal benyttes. Når arbejdet med journaler er afsluttet skal de umiddelbart lægges på plads i arkivet.
Referencer	1. Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (Persondataloven) med eventuelle senere ændringer. 2. Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning med eventuelle senere ændringer. 3. Vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning med eventuelle senere ændringer. 4. Informationssikkerhed – vejledning for sundhedsvæsenet 25. februar 2008. 5. Sundhedsstyrelsens vejledning nr. 161 af 16. september 1998 om information og samtykke og om videregivelse af helbredsoplysninger mv. 6. Lovbekendtgørelse nr. 913 af 13. juli 2010, kap. 5. Bekendtgørelse af sundhedsloven med eventuelle senere ændringer. 7. Bekendtgørelse nr. 665 af 14. september 1998 om information og samtykke og om videregivelse af helbredsoplysninger mv. med eventuelle senere ændringer. 8. Generiske målepunkter for Sundhedsstyrelsens tilsyn med private behandlingssteder.