-

Dokumentation af sikkerhed i forbindelse med databehandling

Al databehandling, der er underlagt persondataloven, skal overholde de tekniske krav, der er opstillet i Datatilsynets bekendtgørelse 528 (sikkerhedsbekendtgørelsen). Skabelonen anvendes til at dokumentere, sikkerhedsforanstaltningerne ved manuel eller elektronisk databehandling.

1. Skema udfyldt af: (Navn + Hospital) **Dato:** **Projektansvarlig (Navn + Hospital)** (samme navn som under pkt. 5 i anmeldelsesskemaet) Skal kun skrives på hvis det ikke er samme person	**Mette Krag, Rigshospitalet** **27.04.2015** **Opdateret: 13.04.2016** **Søren Marker, Rigshospitalet** **Opdateret (uden ændringer i dette dokument): 14.03.17** **Opdateret (uden ændringer i dette dokument): 06.12.17** **Opdateret (uden ændringer i dette dokument): 17.01.18**
2. Databehandlingens id og journalnummer	RH-2015-32 I suite: 03695
3. Databehandlingens titel (kort): Stress Ulcer Prophylaxis in the Intensive Care Unit (SUP-ICU)	

Manuel databehandling	
4. Anvendelse af biobank **NB: såfremt materialet i en forsknings biobank skal anvendes til mere end ét projekt, skal biobanken anmeldes separat.**	☒ Nej ☐ Ja, **biobank** ☐ der oprettes en ny biobank ☐ Forsknings biobank ☐ Klinisk biobank ☐ der anvendes eksisterende biobank Anfør journal nr på biobanks godkendelse_____

Hvem har adgang til biobanken? Kun medarbejdere, som den dataansvarlige bemyndiger hertil, må få adgang til de registrerede informationer.	*Beskriv(f.eks. navne, afdeling):*
Hvordan er biobanken sikret mod uvedkommende? Du er forpligtiget til at opbevare biobanken i henhold til kravene i Sikkerhedsbekendtgørelsen. Lokaler hvor biomaterialet opbevares, skal være aflåst forsvarligt og kun personer, der er bemyndigede, må have adgang. Data skal være pseudoanonymiseret.	*Beskriv:* ☐ *Aflåst fryser* ☐ *Aflåst lokale, lokale nr: afdeling:* ☐ *Pseudoanonymiseret data* ☐ Andet:
Hvordan destrueres biomaterialet? Beskriv kort destruktionsmetoden.	*Beskriv:*
Hvis Biomaterialet skal sendes/videregives til en ekstern databehandler, hvordan sikres der en sikker forsendelse/videregivelse? Beskriv kort hvordan biomaterialet sendes/videregives mellem projektansvarlig og ekstern databehandler. **NB: materialet må ikke udleveres/forsendes/videregives til en ekstern databehandler uden en underskrevet databehandleraftale Ønsker en 3.part at få biologisk materiale, må dette ikke uden videre udleveres. Kontakt den lokale kontaktperson derom.**	*Beskriv:*
5. Anvendelse af flytbare medier Eks: USB stik, USB harddisk, DVD, CD Vær opmærksom på at USB stiks / harddiske skal krypteres. Vær opmærksom på at en bærbar pc IKKE skal noteres her, eftersom der IKKE må ligge forskningsdata direkte på den bærbare pc uanset om den er krypteret eller ej, i henhold til Region Hovedstadens Informationssikkerhedspolitik. Vær OBS på at data der gemmes på flytbare medier ikke kan gendannes/reetableres!	☒ Nej ☐ Ja, **flytbare medier** , hvilke:

Hvem har adgang til de flytbare medier? Kun medarbejdere, som den dataansvarlige bemyndiger hertil, må få adgang til de registrerede data.	*Beskriv(f.eks. navne, afdeling):*
Hvordan er de flytbare medier fysisk sikret mod uvedkommende? Lokaler eller opbevaringspladser, hvor data opbevares, skal være aflåst og kun personer, der er bemyndigede må have adgang.	*Beskriv:*
Hvordan destrueres/slettes de flytbare medier? Beskriv kort metoden.	*Beskriv:*
Hvis et flytbart medie skal sendes/videregives til en ekstern databehandler, hvordan sikres der en sikker forsendelse/videregivelse? Beskriv kort hvordan et flytbart medie sendes/videregives mellem projektansvarlig og ekstern databehandler.	*Beskriv:*
6. Anvendelse af papir materiale Eks: spørgeskemaerne, CRF, samtykke erklæringer m.fl.	☐ Nej ☒ Ja, **papir materiale**
Hvem har adgang til papirmaterialet? Kun medarbejdere, som den dataansvarlige bemyndiger hertil, må få adgang til de registrerede data. Drejer det sig om en længere liste af personer som kan udskiftes i løbet af projektet, kan den dataansvarlige for projektet oprette en liste over bemyndigede. Denne liste skal altid være opdateret og kunne fremsendes på forlangende. Liste skal indeholde navn og organisatorisk tilknytning på personer som aktuelt har adgang eller har haft adgang på et	En til stadighed opdateret liste over bemyndigede personer vil blive opbevaret i et aflåst skab (se nedenfor). Følgende vil have adgang til listen og sikre opdateringen af denne: Mette Krag, Morten Hylander Møller og Søren Marker Intensiv Terapiklinik 4131, Rigshospitalet Blegdamsvej 9 2100 København ☒ Ja, databehandler opretter og vedligeholder en liste over bemyndigede

tidligere tidspunkt, samt det tidsrum de har / har haft adgang.	
Hvordan er papirmaterialet sikret mod uvedkommende? Lokaler eller opbevaringspladser, hvor data opbevares, skal være aflåst og kun personer, der er bemyndigede må have adgang. Data kan være pseudoanonymiseret.	*Beskriv:* Alt papirmateriale med personhenførbare oplysninger opbevares i mappe i aflåst skab (nr. to skab fra venstre i lokale 3104) på Rigshospitalet.
Hvordan destrueres/anonymiseres papirmaterialet? Beskriv kort metoden.	*Beskriv:* Alt papirmateriale makuleres når opbevaringsperioden afsluttes.
Hvis papir materiale skal sendes/videregives til en ekstern databehandler, hvordan sikres der en sikker forsendelse/videregivelse? Beskriv kort hvordan papirmateriale sendes/videregives mellem projektansvarlig og ekstern databehandler.	*Beskriv:* Der foregår ingen forsendelse af papirdokumenter

Elektronisk databehandling

7.a Følgende system(er) anvendes til registrering af data i projektet:

☐ **KMS**
☐ **Analyseportalen**
☐ **SPSS**
☐ **SAS**
☐ **SQL**
☐ **Office (Excel, word, access)**
☐ **Godkendt klinisk eller forsknings web database (SSI/Danske Regioner)**
☒ **Andet?__** web-baseret database med sikret HTTPS forbindelse (udbydes ikke af IMT, men laves af Copenhagen Trial Unit (afdeling på Rigshospitalet)

7.b Data trækkes fra følgende kliniske IT-systemer

☒ **GS!åben /OPUS arbejdsplads**
☒ **EPM**
☒ **ORBIT**
☒ **Labka II**
☒ **RIS/PACS**
☒ **Andet internt system?____CIS (udbydes af IMT)_____**
☒ **Andet eksternt system? _____**

8. Brugeradministrationsløsning: Hvordan valideres brugeren ved login til systemet? "AD" anvendes ved systemer som ikke har et specifik login, men hvor brugeren er logget på regionens netværk, f.eks. Office, SQL, SPSS "BAM" anvendes til flere regionens egne kliniske IT systemer, f.eks. OPUS, ORBIT "Andet" anvendes til IT-systemer som har egen login, herunder IT-systemer som tilgås via en web browser, f.eks. data hostet hos en ekstern leverandør.	☐ **AD** ☒ **BAM** ☒ **Andet (skal besvares hvis der er X ved andet i pkt. 7.a)?__** Brugere administreres af administrator som tildeler personligt brugernavn og login til IT-systemet som tilgås via en web browser med sikker HTTPS forbindelse **_____**
9. Typer af brugere: Her må gerne noteres navngivne personer, hvis de er kendte. Drejer det sig om en hel afdeling så skriv navnet på afdelingen. Her skal også noteres hvis der er eksterne leverandører der skal have adgang typisk som systemadministratorer.	☒ Ja, alm. brugere, hvem?_____ ☐ Ja, superbrugere, hvem?_____ ☒ Ja, systemadministratorer, hvem?__ Projektansvarlig: Morten Hylander Møller Intensiv terapi klinik, Rigshospitalet morten.hylander.moeller@regionh.dk Tlf.: 3545 8685

	Koordinerende investigator: Læge klinisk assistent Mette Krag Intensiv terapi klinik, Rigshospitalet mette.krag.01@regionh.dk Tlf.: 42405714 Læge og klinisk assistent Søren Marker Intensiv terapi klinik, Rigshospitalet soeren.marker.jensen.01@regionh.dk Tlf: 35457450 Forskningssygeplejersker på Intensiv terapi klinik, Rigshospitalet Systemadministrator på CTU Data manager Janus Engstrøm Copenhagen Trial Unit (CTU), Rigshospitalet janus@ctu.dk Tlf.: 3545 7161 ☐ Ja, andre, hvem?_____
10. Rettigheder: Det er et krav, at it-løsningen kan skelne mellem brugernes rettigheder. • Læse • Skrive • Rette • Slette • Systemadministratoradgang Der skal kunne foretages kontrol af tildelte rettigheder mindst hvert halve år. Hvor og hvordan kan informationer om de enkelte brugers rettigheder samt foretagne kontroller tilgås?	**Skal kun udfyldes hvis der i pkt. 8 er sat kryds i "Andet"!** *Alm. bruger* Alm. Bruger og kan læse og skrive data på patienter, som er inkluderet på ens egen afdeling. *Systemadministrator* Oprettelse af lande, hospitaler og brugere i systemet. Administration af ovenstående. Adgang til logs (kan ikke redigeres). Sletning af patientdata, hvis samtykke trækkes tilbage. Udtræk fra database. Adgangen omfatter hele systemet og ikke kun et enkelt hospital.
11. Login-procedure: Kun autoriserede brugere må have adgang til it-løsningen. Alle brugere skal have en personlig adgangskode, der følger regionens retningslinjer. Hvis det er muligt at tilgå it-løsningen udenom login-proceduren, skal det beskrives, hvem der har disse rettigheder, og hvordan man håndterer disse.	**Skal kun udfyldes hvis der i pkt. 8 er sat kryds i "Andet"!** Hver bruger oprettes med brugernavn og personlig adgangskode, der består af mindst 8 karakterer og indeholder små bogstaver, store bogstaver og tal. Adgangskoden kan ændres af bruger såfremt den opfylder ovenstående krav.

12. Brugeroplysninger: Det er et krav, at man entydigt kan identificere en bruger, Hvilke oplysninger registreres der om brugerne? • Navn • CPR-nummer • Brugernavn • Organisatorisk tilknytning	**Skal kun udfyldes hvis der i pkt. 8 er sat kryds i "Andet"!** Navn Stilling Organisatorisk tilknytning Kontaktoplysninger – registreres på alle brugere
13. Adgangskontrol og -log: Der skal kunne udskrives en adgangslog med angivelse af, hvem der har haft adgang til IT-løsningen og på hvilke tidspunkt Efter fem afviste adgangsforsøg fra samme arbejdsstation eller samme bruger-id skal der blokeres for flere forsøg. Der skal ske en løbende opfølgning på afviste adgangsforsøg.	**Skal kun udfyldes hvis der i pkt. 8 er sat kryds i "Andet"!** Adgangslog indeholder dato, tid, bruger, kort beskrivelse af hændelse f.eks. login, logout, spærring af konto, mislykket login. Efter 5 afviste adgangsforsøg spærres kontoen. Administrator har adgang til adgangslog og vil følge op på spærrede konti samt have mulighed for at genåbne kontoen.
14. Transaktionslog: Det er et krav, at der fra systemet kan udskrives en transaktionslog, som indeholder disse oplysninger: • Bruger • Organisatorisk tilknytning • Hvilken af systemets funktioner der har været anvendt • Tidspunkt • CPR-nummer på person der er arbejdet med eller • Udtrækskriterie, hvis der er søgt på flere personer NB: Hvis der er tale om forskning eller statistik, kan der afviges fra kravet om transaktionslog, såfremt identifikationsoplysningerne for personen enten er krypterede eller kodede f.eks. via en omsætningsnøgle (pseudoanonymiserede).	☒ Ja, transaktionslog, samtlige punkter i venstre side logges. *VIGTIGT: Som udgangspunkt skal du oprette en omsætningsnøgle- da der kun er meget få systemer der kan danne en transaktionslog som overholder lovgivningen (f.eks. KMS, Analyse og muligvis SQL).* Systemet har transaktionslog. Administrator vil kunne se, hvilken patients data brugeren har arbejdet med. Loggen vil sikre, at hvert eneste element af brugertastede data i databasen kan spores til den bruger, der indtastede det, hvilken patient der er indtastet på og hvornår indtastningen er foretaget. Det er ikke muligt for alm. brugere at lave søgninger på patienter i databasen. Patienter inkluderet på brugerens eget hospital vil blive vist på en liste i databasen og det vil ikke være muligt at se data for andre patienter. ☐ Nej, men der oprettes en omsætningsnøgle eller lignende, som opbevares adskilt fra projektets data på:_____
15. Opbevaring af logge:	**Skal kun udfyldes hvis der i pkt. 8 er sat**

En log skal og må opbevares i seks måneder. Hvordan opbevares loggen? Hvordan kan man fremfinde information fra loggen?	**kryds i "Andet"!** Loggen opbevares på server I 6 måneder og slettes herefter: Loggen opbevares på server (den samme som databasen opbevares på): DNS-navn: oc.ctu.dk Lokalisation: Copenhagen Trial Unit. Rigshospitalet Tagensvej 22, 2200 Kbh. N, kælderen, Rum K128A (eneste server i rummet) Kontaktperson: Janus Engstrøm Tlf.: 3545 7161 Email: janus@ctu.dk
16. Overførsel af elektronisk data: *Til ekstern databehandler:* Her skal beskrives, hvordan det sikres at data der overføres elektronisk til en person / et IT-system udenfor den organisatoriske Region Hovedstad, overføres sikkert. F.eks.: Anvendes HTTPS, kryptering, andet? *Til interne projektdeltagere:* Data bør i udgangspunktet ikke overføres elektronisk mellem 2 ansatte i Region Hovedstaden. Data bør placeres på et netværksdrev der sikre at alle deltagere kan tilgå data. (se også pkt. 18) Hvis data alligevel skal overføres elektronisk skal det beskrives hvorledes det sikres.	☐ Nej, ingen overførsel af elektronisk data ☒ Ja, data overføres elektronisk, beskriv: Data overføres via sikker forbindelse (HTTPS) til server. Til overførsler mellem interne projektdeltagere vil der blive brugt en lukket mappe på V-drevet, som kun projektdeltagere vil have adgang til.
17. Eksterne kommunikations-forbindelser ind i vores netværk: *Inddata:* Her skal beskrives, hvordan det sikres at uvedkommende ikke får adgang i tilfælde af at der er eksterne kommunikations-forbindelser til systemet eller regionens netværk. F.eks.: En leverandøradgang.	☒ Nej, ingen eksterne kommunikationsforbindelser ☐ Ja, en virksomhed, leverandør eller person skal have adgang til vores netværk, beskriv:

18. Brugeradgange og databehandling uden for Region Hovedstadens lokaliteter: Hvis der for brugeren sker behandling af personoplysninger uden for Region Hovedstadens lokaliteter, fx en hjemmearbejdsplads, skal databehandlingen overholde regionens retningslinjer for anvendelse af fjernarbejdspladser.	☒ Nej, ☐ Ja, dette sker via en sikker forbindelse, som er sat op og administreret af CIMT
Hvis det er en sikker forbindelse sat op af en ekstern part, skal det anføres hvor den er sikret? F.eks.: Anvendes HTTPS, VPN, andet?	☒ Ja, dette sker via en sikker forbindelse, som er sat op og administreret af en leverandør (herunder sundhedsdatanettet) Hvordan er forbindelsen sikret? ☒ HTTPS ☐ VPN ☐ Andet, beskriv:
19. Fysiske forhold Intern Hvor er IT-løsningen/databasen placeret? (f.eks. på H:\, P:\ eller andet drev) Opbevaring af data skal ske på en sådan måde, at uvedkommende ikke kan få adgang. Ligeledes skal det sikres, at inddatering mv. ikke foregår et sted, hvor uvedkommende kan få adgang til at se data. Vær opmærksom på at databaser (Access, SQL, SPSS, SAS m.v.) ikke må ligge på et personligt drev (typisk H:\ drevet). **P:\ drev** – afdelingsdrev – deling af data i samme afdeling **V:\ drev** – virksomhedsdrev – deling af data i samme virksomhed / hospital **R:\ drev** – regionsdrev / deling af data i regionen på tværs af virksomheder/hospitaler	**For hvert kryds skriv: navn på mappen samt hvad der ligger i mappen, hvis flere mapper på samme drev skal det skrives tydeligt.** ☐ H:\ ☐ P:\ - i adgangsbegrænset mappe af CIMT ved navn:…… ☒ V:\ - i adgangsbegrænset mappe af CIMT ved navn:…… ☐ R:\Tværgående Forskning - i adgangsbegrænset mappe af CIMT ved navn:…… ☒ Andet internt: navn: oc.ctu.dk DNS-navn: oc.ctu.dk databasen opbevares på server: Lokalisation: Copenhagen Trial Unit. Rigshospitalet Tagensvej 22, 2200 Kbh N, kælderen, Rum K128A (eneste server i rummet) Kontaktperson: Janus Engstrøm Tlf.: 3545 7161 Email: janus@ctu.dk

20. Fysiske forhold Ekstern Hvis data er placeret hos en ekstern leverandør eks. at data hostes, skal det markeres her, og følgende skal beskrives: *Vær opmærksom på at dette kræver at der er markeret at der er en ekstern databehandler i anmeldelsesskemaet, samt at der underskrives en databehandleraftale.* *Det kan også kræve at leverandøren skal udfylde et leverandørvurderingsskema.*	☒ Nej, ingen ekstern placering af data ☐ Ja, andet ekstern: (navn)
Hvordan sendes /overføres data til leverandøren? F.eks.: Data indtastes via en sikker web site; Data placeres midlertidigt på en krypteret usb-stik, som slettes når data er overført.	*Beskriv:*
Hvordan sikrer leverandøren og den projektansvarlige at data slettes ved projektets afslutning? Slettes data på et forudbestemt tidspunkt, eller skal den projektansvarlige give besked? Hvilken metode anvender leverandøren til at slette data? Sender leverandøren en rapport/besked om at data er slettet?	*Beskriv:*
21. Andre væsentlige oplysninger vedr. databehandlingen: Det elektroniske system OpenClinica vil blive benyttet. OpenClinica er udviklet specifikt med henblik på datafangst i større forskningsprojekter. Ændring i personkredsen godkendt, Kirsten Ingrid Lindeblad, Jur.Enhed, Rigshospitalet, 26. april 2017.	

Anmeldelse af databehandling sker i henhold til fælles sikkerhedsbestemmelser for Region Hovedstaden vedrørende behandling af personoplysninger i henhold til Persondataloven, vedtaget af Regionsrådet d. 24. april 2007 og senest revideret juli 2012.