Databehandler aftale

Nærværende aftale beskriver vilkår og betingelser for håndtering af personfølsomme patient- og fakturadata hos Digifys.com.

Databehandleren (Digifys.com) handler alene efter instruks fra den dataansvarlige (kunden).

Databehandleren træffer de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.

Databehandleren skal på den dataansvarliges anmodning give den dataansvarlige tilstrækkelige oplysninger til, at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

Yderemere overholdes reglerne for databehandling i sikkerhedsbekendtgørelsen til beskyttelse af personoplysninger i den offentlige forvaltning (se bilag).

Sikkerhedsforanstaltningerne på Digifys.com er beskrevet særskilt

Digifys.com kan fuldt integreres med de administrative systemer; Complimenta, X-dont og Equus - såfremt den dataansvarlige med sin underskrift herunder giver samtykke hertil.

Dato

14/8 2017 14/8-17

Underskrift kunde

Underskrift Digifys

Sikkerhedsforanstaltninger til beskyttelse af personoplysninger i Digifys

Digifys's systemportefølje er for det første produkter, der udelukkende tilgås via internettet. For det andet indeholder systemet proprietære APP's udviklet til iPhone/iPad.

Sikkerhedsforanstaltninger i www-løsningerne

Kommunikation over internettet

Al kommunikation over internettet sker via krypteret dataoverførsel.

Digifys kører med https/SSL-kryptering.

Autorisation og adgangskontrol

Digifys kan kun tilgås af personer med korrekt adgangskode og password.

En bruger er identificeret via sin e-mailadresse. Brugere opretter selv, via et tidsbegrænset hyperlink, deres password inde på sitet. Passwordet skal bestå af mindst 8 karakterer og indeholde både bogstaver og tal.

Såfremt en bruger glemmer sit password kan et nyt password bestilles, hvorved processen med oprettelse af password gentages.

Administrative brugere fjernes fra systemet, såfremt stopper hos Digifys eller af anden årsag ikke anvender deres bruger ID indenfor en 6 måneders periode.

Overvågning af forsøg på uretmæssig systemadgang

Domainbox foretager overordnet overvågning af netværket, herunder angreb af forskellig art. Det være sig DDoS-angreb, Brute force-angreb, botnet-aktivitet eller forsøg på inficering af websider på netværket ved for eksempel fjern-inklusion af malware og lignende.

Derudover foregår der konstant overvågning af serveren ved hjælp af værktøjer, der måler trafikmængde, forespørgsler og ydeevne. Ved atypiske mønstre notificeres serveradministratorer. Dette er med til at forebygge og forhindre forsøg på uretmæssig adgang.

Ved forgæves loginforsøg låses konti automatisk, ligesom der i databasen opbevares optegnelser over forgæves loginforsøg.

Omfang af adgang

En klinikejer tildeler autorisation til de enkelte fysioterapeuter på den enkelte klinik.

En fysioterapeut har adgang til patienter tilhørende klinikken han arbejder på.

En patient har udelukkende adgang til data vedrørende patienten selv.

En klinikejer kan udtrække statistik på data for sin klinik.

En samling af klinikker kan efter nærmere aftale tildele retten til at udtrække statistik til Digifys ApS eller til en tredjepart.

Digifys-administrative brugere (interne brugere) har adgang til alle brugeres data.

Sikkerhedskopiering

Der foretages dagligt sikkerhedskopiering af data liggende i Digifys-systemportefølje. Dette gælder både databaser og filer, således at eventuel mistet data vil kunne genskabes. Sikkerhedskopieringer foretages både til en lokal backup-server og til en fjernlokation (remote).

Sikkerhedsforanstaltninger i APP's

Digifys har udviklet 2 APP's til sine brugere. Den ene er til fysioterapeuterne og bruges til optagelse af egne øvelser som uploades til systemet. Den anden er til patienten og bruges af denne til at se de øvelser fysioterapeuten har givet, samt til af rapportere informationer om træningen tilbage til fysioterapeuten.

APP til optagelse af egne videofilm

Den enkelte fysioterapeut kan optage nye videoøvelser som kan anvendes til programlægning til patienter via sin iPhone/iPad. Efter optagelse af den enkelte video kategoriseres videoen med en række karakteristika, der hjælper indplacering i strukturen af videoøvelser i Digifys.

De enkelte videoer samt kommunikationen med www.digifys.com indeholder ingen persondata, udelukkende filmen samt kategori-informationer, samt krypterede login-informationer. Digifys anbefaler endvidere at upload foregår via firewall-sikrede wifi-netværk.

Når den enkelte video er overført til Digifys, er sikkerhedsforanstaltningerne i www-løsningen dækkende.

APP til rapportering af data i forbindelse med udførsel af øvelser

Patienten kan via sin App logge ind og se sit program på sin iPhone/iPad. Al data overføres krypteret.

Patienten kan efter udførsel af sit program tilbagerapportere, eksempelvis hvor mange gentagelser han har gennemført af den enkelte øvelse samt hvordan han følte sig under og efter gennemførslen. Udførselsdata overføres ligeledes krypteret tilbage til www.digifys.com

IT-revision

Digifys hostes af Domainbox ApS, som er underlagt revision af BDO Statsautoriseret aktieselskab.

Som en del af revisionen af et årsregnskab vurderer BDO de risici, som anvendelsen af it indebærer i forhold til regnskabet, og hvordan virksomheden har reageret herpå ved at indføre interne kontroller.

I kontrollen af selskabet vurderer BDO, om forsvarlige procedurer er implementerede inden for drift, adgangssikkerhed samt anskaffelse og vedligeholdelse af it-systemer.

It-revision omfatter også en undersøgelse og vurdering af, om det er muligt at fortsætte forretningsdriften i tilfælde af en katastrofe eller et kritisk it-nedbrud, og om relevant lovgivning og regulativer overholdes.

Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

I medfør af § 41, stk. 5, i lov nr. 429 af 31. maj 2000 om behandling af personoplysninger fastsættes:

Kapitel 1

Almindelige bestemmelser

§ 1. Denne bekendtgørelse gælder for behandling af personoplysninger, som foretages for den offentlige forvaltning helt eller delvis ved hjælp af elektronisk databehandling.

§ 2. Behandling af personoplysninger skal ske i overensstemmelse med bestemmelserne i kapitel 1 og 2.

Stk. 2. Behandling af personoplysninger, hvor der skal ske anmeldelse til Datatilsynet efter reglerne i kapitel 12 i lov om behandling af personoplysninger, skal tillige ske i overensstemmelse med bestemmelserne i denne bekendtgørelses kapitel 3. Dette gælder dog ikke for behandling af personoplysninger, der udelukkende sker med henblik på at føre et retsinformationssystem, i det omfang der er tale om oplysninger i den offentligt tilgængelige del af retsinformationssystemet.

§ 3. Den dataansvarlige myndighed skal træffe de fornødne tekniske og organisatoriske foranstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.

Stk. 2. For personoplysninger, som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

§ 4. Datatilsynet fører tilsyn med overholdelsen af denne bekendtgørelse og kan i den forbindelse komme med henstillinger over for den dataansvarlige myndighed vedrørende de trufne sikkerhedsforanstaltninger, jf. § 3.

Kapitel 2

Generelle sikkerhedsbestemmelser

§ 5. Den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de

regler, der fremgår af denne bekendtgørelse. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

Stk. 2. De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i myndigheden.

§ 6. Den dataansvarlige myndighed skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. Medarbejderne skal herunder gøres bekendt med de regler, der er fastsat i medfør af § 5.

§ 7. Hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal der foreligge en skriftlig aftale, hvoraf det fremgår, at reglerne i denne bekendtgørelse ligeledes gælder for behandlingen ved databehandleren. Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne.

Stk. 2. Hvis behandling af personoplysninger finder sted på en pc-arbejdsplads uden for den dataansvarlige myndigheds lokaliteter, skal myndigheden fastsætte særlige retningslinier herfor, således at det sikres, at bestemmelserne om sikkerhedsforanstaltninger iagttages.

§ 8. På steder, hvor der foretages behandling af personoplysninger, skal der træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.

§ 9. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes de fornødne foranstaltninger for at sikre, at bestemmelsen i § 3 iagttages.

Inddatamateriale som indeholder personoplysninger

§ 10. Inddatamateriale, som ikke indgår i en manuel sag eller i et manuelt register, må kun anvendes af personer, som er beskæftiget med inddatering. Inddatamateriale, som er omfattet af bestemmelsen i § 2, stk. 2, skal opbevares aflåst, når det ikke anvendes.

Stk. 2. Inddatamateriale som nævnt i stk. 1 skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, eller til

kontrol med de inddaterede personoplysninger, dog senest efter en af den dataansvarlige myndighed nærmere fastsat frist.

Stk. 3. Ved tilintetgørelse af inddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

Autorisation og adgangskontrol

§ 11. Kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles.

Stk. 2. Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

Stk. 3. Der må endvidere autoriseres personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

§ 12. Der skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

Uddatamateriale som indeholder personoplysninger

§ 13. Uddatamateriale må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages.

Stk. 2. Herudover må uddatamateriale anvendes af personer, som er beskæftiget med revision eller drifts- og systemtekniske opgaver i det pågældende system.

Stk. 3. Uddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt heri.

Stk. 4. Uddatamateriale skal slettes eller tilintetgøres, når det ikke længere skal anvendes til de formål, som behandlingen varetager, og senest efter en af den dataansvarlige myndighed nærmere fastsat frist.

Stk. 5. Ved tilintetgørelse af uddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger mod, at materialet misbruges eller kommer til uvedkommendes kendskab.

Stk. 6. Bestemmelserne i stk. 1-5 gælder ikke for uddatamateriale, som indgår i en manuel sag eller i et manuelt register.

Eksterne kommunikationsforbindelser

§ 14. Der må kun etableres eksterne kommunikationsforbindelser, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

Kapitel 3

Supplerende sikkerhedsforanstaltninger for anmeldelsespligtige behandlinger

§ 15. Bestemmelserne i kapitel 3 finder ikke anvendelse i det omfang de behandlede oplysninger ikke i sig selv ville være omfattet af anmeldelsespligt til Datatilsynet.

Autorisation og adgangskontrol

§ 16. Autorisationer, jf. § 11, skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.

§ 17. Det skal sikres, at de autoriserede personer fortsat opfylder betingelserne i § 11, stk. 2 og 3, og § 16.

Stk. 2. Kontrol heraf skal foretages mindst en gang hvert halve år.

Kontrol med afviste adgangsforsøg

§ 18. Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg. Der skal løbende ske opfølgning i myndigheden.

Logning

§ 19. Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Stk. 2. Bestemmelsen i stk. 1 finder ikke anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for en af den dataansvarlige myndighed nærmere fastsat kortere frist.

Stk. 3. Bestemmelsen i stk. 1 finder ikke anvendelse, hvis behandlingen af personoplysninger udelukkende sker ved afvikling af programmer, som foretager en forud defineret massebehandling af personoplysninger (»batch»-kørsler). Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

Stk. 4. Bestemmelsen i stk. 1 finder endvidere ikke anvendelse, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

Stk. 5. Bestemmelsen i stk. 1 finder endelig ikke anvendelse for personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfatter tillige personoplysninger, som manuelt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger.

Kapitel 4

Ikrafttræden

§ 20. Bekendtgørelsen træder i kraft den 1. juli 2000.

Justitsministeriet, den 15. juni 2000

Frank Jensen