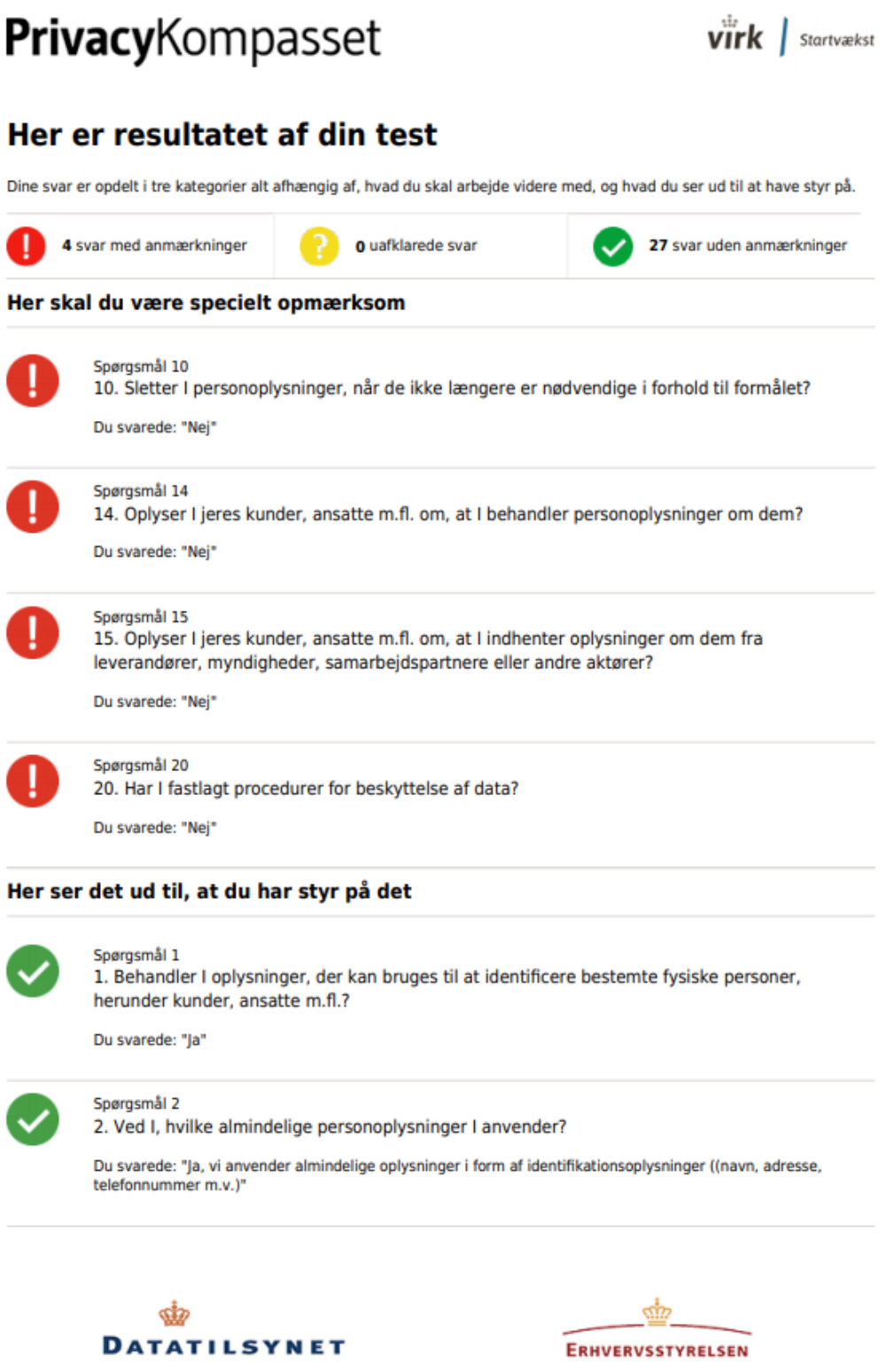

PrivacyKompasset

virk | Startvækst

Her er resultatet af din test

Dine svar er opdelt i tre kategorier alt afhængig af, hvad du skal arbejde videre med, og hvad du ser ud til at have styr på.

4 svar med anmærkninger | **0** uafklarede svar | **27** svar uden anmærkninger

Her skal du være specielt opmærksom

Spørgsmål 10
10. Sletter I personoplysninger, når de ikke længere er nødvendige i forhold til formålet?

Du svarede: "Nej"

Spørgsmål 14
14. Oplyser I jeres kunder, ansatte m.fl. om, at I behandler personoplysninger om dem?

Du svarede: "Nej"

Spørgsmål 15
15. Oplyser I jeres kunder, ansatte m.fl. om, at I indhenter oplysninger om dem fra leverandører, myndigheder, samarbejdspartnere eller andre aktører?

Du svarede: "Nej"

Spørgsmål 20
20. Har I fastlagt procedurer for beskyttelse af data?

Du svarede: "Nej"

Her ser det ud til, at du har styr på det

Spørgsmål 1
1. Behandler I oplysninger, der kan bruges til at identificere bestemte fysiske personer, herunder kunder, ansatte m.fl.?

Du svarede: "Ja"

Spørgsmål 2
2. Ved I, hvilke almindelige personoplysninger I anvender?

Du svarede: "Ja, vi anvender almindelige oplysninger i form af identifikationsoplysninger ((navn, adresse, telefonnummer m.v.)"

DATATILSYNET

ERHVERVSSTYRELSEN

PrivacyKompasset

virk | Startvækst

Spørgsmål 2
2. Ved I, hvilke almindelige personoplysninger I anvender?

Du svarede: "Ja, vi anvender betalingsoplysninger (kundenummer, pris, vare, kortnummer m.v.)"

Spørgsmål 2
2. Ved I, hvilke almindelige personoplysninger I anvender?

Du svarede: "Ja, vi anvender rekrutteringsoplysninger (uddannelse, tidligere beskæftigelse, stillingsbetegnelse)"

Spørgsmål 2
2. Ved I, hvilke almindelige personoplysninger I anvender?

Du svarede: "Ja, vi anvender CPR-numre"

Spørgsmål 2
2. Ved I, hvilke almindelige personoplysninger I anvender?

Du svarede: "Ja, vi anvender andre almindelige personoplysninger"

Spørgsmål 3
3. Ved I, hvilke følsomme personoplysninger I anvender?

Du svarede: "Ja, vi anvender helbredsoplysninger (sygemelding og årsagen hertil, køb af bestemt medicin m.v.)"

Spørgsmål 3
3. Ved I, hvilke følsomme personoplysninger I anvender?

Du svarede: "Ja, vi anvender andre følsomme personoplysninger"

Spørgsmål 4
4. Til hvilke bestemte formål indsamler og opbevarer I personoplysninger?

Du svarede: "Personaleadministration om ansatte samt ansøgere til stillinger."

Spørgsmål 4
4. Til hvilke bestemte formål indsamler og opbevarer I personoplysninger?

Du svarede: "Køb, salg og levering af produkter eller tjenester."

Spørgsmål 4
4. Til hvilke bestemte formål indsamler og opbevarer I personoplysninger?

Du svarede: "Markedsføring"

DATATILSYNET

ERHVERVSSTYRELSEN

FYSIO DANMARK

PrivacyKompasset

virk | Startvækst

Spørgsmål 5
5. Er de personoplysninger, I behandler, begrænset til det, der er nødvendigt i forhold til jeres formål med behandlingen?

Du svarede: "Ja"

Spørgsmål 6
6. Anvender I personoplysninger til et andet formål end det, oplysningerne blev indsamlet til?

Du svarede: "Nej"

Spørgsmål 7
7. Har I et lovligt grundlag for jeres behandling af almindelige personoplysninger?

Du svarede: "Ja, for de almindelige personoplysninger er det nødvendigt for, at vi kan forfølge en legitim interesse, som er vigtigere end hensynet kunderne, ansatte m.fl.

Spørgsmål 8
8. Har I et lovligt grundlag for jeres behandling af følsomme personoplysninger?

Du svarede: "Ja, det er nødvendigt for, at vi kan beskytte den registreredes vitale interesser"

Spørgsmål 8
8. Har I et lovligt grundlag for jeres behandling af følsomme personoplysninger?

Du svarede: "Ja, det er nødvendigt for, at vi kan varetage et retskrav"

Spørgsmål 9
9. Sørger I for at opdatere de personoplysninger, I behandler?

Du svarede: "Ja"

Spørgsmål 11
11. Har I et grundlag for at videregive oplysninger om jeres ansatte, kunder m.fl. til samarbejdspartnere eller andre aktører?

Du svarede: "Ja"

Spørgsmål 12
12. Overfører I personoplysninger til samarbejdspartnere i tredjelande?

Du svarede: "Nej"

Spørgsmål 13
13. Giver I jeres kunder, ansatte m.fl. jeres kontaktoplysninger?

Du svarede: "Ja"

DATATILSYNET

ERHVERVSSTYRELSEN

FYSIO DANMARK

PrivacyKompasset

virk | Startvækst

Spørgsmål 16
16. Kan jeres kunder, ansatte m.fl. få en kopi af de personoplysninger, I opbevarer om dem?

Du svarede: "Ja"

Spørgsmål 17
17. Kan jeres kunder, ansatte m.fl. få rettet, slettet eller blokeret deres personoplysninger, når indholdet er urigtigt?

Du svarede: "Ja"

Spørgsmål 18
18. Kan jeres kunder, ansatte m.fl. gøre indsigelse mod jeres behandling af deres personoplysninger?

Du svarede: "Ja"

Spørgsmål 19
19. Giver I mulighed for, at jeres kunder kan overføre deres personoplysninger til en anden virksomhed?

Du svarede: "Ja"

Spørgsmål 21
21. Har I udpeget en databeskyttelsesrådgiver (DPO)?

Du svarede: "Vi skal ikke udpege en DPO"

Spørgsmål 22
22. Hvis I har en hjemmeside, oplyser I så brugerne af hjemmesiden om formålet med at placere cookies på deres udstyr?

Du svarede: "Ja, vi oplyser om formål og relevans, når vi placerer cookies"

Spørgsmål 23
23. Indhenter I jeres hjemmesidebrugeres samtykke, hvis I placerer cookies på deres udstyr?

Du svarede: "Ja"

DATATILSYNET

ERHVERVSSTYRELSEN

FYSIO DANMARK

Svar på spørgsmål fra Screening med PrivacyKompasset hvor FysioDanmark Hillerød, Hørsholm & Lyngby (FDHI) skal være særlig opmærksom.

Spørgsmål 10 - Sletter I personoplysninger, når de ikke længere er nødvendige i forhold til formålet?

Personale:

FDHI opbevarer alle nye (efter den 1.1.2018) personale kontrakter osv. elektronisk i OneDrive - hvor data bliver slettet 5 år efter en medarbejder fratræder. Alle ikke relevante oplysninger slettes efter 3-6 måneder.

Alle kontrakter fra før 1.1.2018 opbevares i papirform i backoffice hvor kun betroede medarbejdere har adgang. Disse kontrakter vil i løbet af 2018 blive indscannet til OneDrive, og slettes som ovenfor nævnt.

Patienter (fysioterapien & virksomhedskunder):

Journalføring foregår udelukkende elektronisk i DigiFys og Geckobooking. En journal opbevares i det tidsrum, der er fastlagt af Styrelsen for Patientsikkerhed. Det gældende tidsrum er 5 år fra det seneste notat i journalen, jf. journalbekendtgørelsens § 15, stk. 2. I særlige tilfælde kan journalen opbevares længere. Til oplysninger til brug for afregningsformål, benyttes Complimenta, her opbevares oplysningerne så længe, det er nødvendigt af hensyn til afregning og bogføring. GDPR for Complimenta er vedhæftet som bilag 1.

Se også FysioDanmark FDHI Persondata politik.

GDPR for DigiFys og Geckobooking er vedhæftet som bilag 2 og 3.

Kunder (fitness):

FDHI opbevarer alle nye (efter den 1.6.2018) kunde kontrakter osv. elektronisk i OneDrive. I kontrakten gives der samtykke til opbevaring efter endt medlemskab samt til brug af billeder der er taget i centeret.

Alle kontrakter fra før 1.6.2018 opbevares i papirform i backoffice hvor kun betroede medarbejdere har adgang. Disse kontrakter vil i løbet af 2018 blive indscannet til OneDrive. Vores udbyder Sport Solution er ved at udarbejde en elektronisk samtykkeerklæring der kan bruges til alle medlemskaber der tidligere er oprettet og samt de fremadrettede.

Spørgsmål 14 - Oplyser I jeres kunder, ansatte m.fl. om, at I behandler personoplysninger om dem?

Dette har vi ikke tidligere gjort, men efter den 1.6.2018 er dette indført.

Spørgsmål 15 - Oplyser I jeres kunder, ansatte m.fl. om, at I indhenter oplysninger om dem fra leverandører, myndigheder, samarbejdspartnere eller andre aktører?

Personale:

FDHI indhenter oplysninger om en medarbejder fra skat i forbindelse med løn.

Patienter (fysioterapien & virksomhedskunder):

FDHI indhenter oplysninger fra Refhost (henvisningshotellet), FDHI informerer patienten i telefonen når vi aftaler et forløb at vi nedhenter henvisningen. FDHI modtager visitation fra forsikringsselskaber - dette er patienten informeret om fra forsikringsselskaberne side af, alternativt kommer patienten selv med visitationen. Det beskrevne er nødvendigheder for at vi kan opfylde erhvervet som sundhedsfaglig virksomhed.

Kunder (fitness):

Betalingsoplysninger til betaling af medlemskab, indtaster kunden selv via et link der bliver sendt til dem under oprettelsen af medlemskabet. Vores leverandør deler disse oplysninger med den altid aktive betalingsoperatør (Nets, Elavon, GoAppified etc.). Der henvises til ”Databehandleraftalen” fra altid aktiv leverandør af softwaren, som er vedhæftet som bilag 4.

Informationen der benyttes til brug af Precore og eGym træningsudstyr er beskyttet via disses GDPR beskrivelser, hvor den enkelte kunde selv skal give deres samtykke til brug af ens personlige data. Se bilag 5 og 6.

Spørgsmål 20 - Har I fastlagt procedurer for beskyttelse af data?

Alle computere har installeret virus beskyttelse, online version der opdateres løbende og scanner løbende maskinen. Alle medarbejdere er oplyst at de skal logge af computeren, når de forlader den. Som ekstra sikkerhed hertil logger computeren automatisk af efter ikke at være benyttet i 5 minutter.

I forbindelse med hjemmearbejdsplads, gælder de samme procedure som på arbejdspladsen.

Ved udskiftning af computer destrueres den gamle harddisk.

Der benyttes personlige adgangskoder til alle systemer og medarbejderne er oplyst om ikke at dele deres adgangskoder. Disse koder er opsat til automatisk at skulle ændres halvårligt. Alle koder skal være på mindst 8 cifre og indeholde både tal og bogstaver.

Alle mails med personfølsomme oplysninger slettes når de ikke længere er relevante. Virksomheden anvender Microsoft Office 365 og har indhentet dennes GDPR der er vedhæftet som bilag 7.

Spørgsmål 21 - Har I udpeget en databeskyttelsesrådgiver (DPO)?

Det er ikke nødvendigt at udpege en DPO da FDHI ikke er omfattet af reglerne for DPO.

Spørgsmål 22

SSL er tvangsaktiveret, således at siden nu kun kan tilgås i krypteret form. Altså med grøn hængelås.

Formularerne på både Hillerød og Lyngby er nu sat til IKKE at gemme i databasen. Det indebærer at den krypterede formular udelukkende sender til jeres mail. Usikkerheden ligger med andre ord i jeres mailhåndtering.

Cookiepolitik, er oprettet og der bruger en ordlyd alla dette:

http://minecookies.org/skabelon-til-cookie-og-privatlivspolitik/

Og jeg bruger teknik herfra:

https://cookieconsent.insites.com/download/

Personale administration

Krav om datasikkerhed i forbindelse med personaleadministration

I forbindelse med personaleadministration skal persondatalovens regler i det hele iagttages. Det indebærer bl.a., at den dataansvarlige virksomhed skal leve op til lovens krav om datasikkerhed.

Der skal træffes 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 loven. Dette følger af lovens § 41, stk. 3.

Datatilsynet har udformet nedenstående specifikke minimumskrav for sikkerhed i forbindelse med personaleadministration. Fra januar 2015 indeholder Datatilsynets tilladelser til personaleadministration i den private sektor som standard vilkår om iagttagelse af disse.

Minimumskrav for sikkerhed i forbindelse med personaleadministration:

1. Beskriv hvordan I beskytter jeres personaleoplysninger i personaleadministration og i praksis har implementeret pkt. 2-12. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.

2. Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.	Ejere og bogholder har adgang til ansættelseskontrakter, og den enkelte medarbejder har fysisk fået udleveret et underskrevet eksemplar.
3. Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.	Dette er kun Ejere og bogholder der har disse beføjelser.
4. Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug. Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.	Kontrakter fra før 1.1.2018 opbevares fysisk på bogholders kontor. Disse bliver i løbet af 2018 indscannet og herefter makuleret, indtil da opbevares de aflåst når bogholder ikke er til stede. Det er kun betroede medarbejdere med tavshedspligt der har adgang til dette kontor. Der benyttes virksomhedens egen krydsmakulatur

5. Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode. De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den. Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.	Alle pc'er og systemer er beskyttet med mindst 8 ciffrede koder. Disse koder er opsat til automatisk at skulle ændres halvårligt. Alle fysioterapeuter har adgang til patientjournaler, det trackes hvem der har adgang til patientjournaler. Sekretærer har ligeledes samme adgang - de er ikke sundhedsfaglige men har tavshedspligt beskrevet i ansættelsesbevis. Ingen har koderne liggende på skrift.
6. Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.	I patientsystemet blokeres adgang ved mere end 5 forgæves forsøg. Alle computere har ikke denne mulighed, men der skal anvendes yderligere koder for at gå på systemer med personfølsomme oplysninger, hvor der blokeres for adgang ved 5 mislykkedes forsøg (arbejdes på fra systemleverandør).
7. Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.	Dette sker ikke da alle oplysninger opbevares krypteret i skyen: Complimenta & DigiFys (Patienter) / FlexyBox & OneDrive (Fitnesskunder) / OnDrive (personale).
8. PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.	Avira eller Awast er instaleret på alle pc'er
9. Hvis der benyttes hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.	Er i gang med at undersøge hvordan en kryptering skal fungere.
10. Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.	Der sendes ikke e-mails med disse oplysninger. Alle medarbejdere er oplyst at der kun må benyttes fornavn og fødselsdato.
11. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.	Alle computere forsøges repareret af Ejer, hvis den ikke ødelægges harddisken inden aflevering på genbrugsplads.
12. Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller rekrutteringssystem på internettet.	Følgende databehandler aftaler er der indhentet: Complimenta & DigiFys (Patienter) FlexyBox & OneDrive (Fitnesskunder) OnDrive (personale). Refhost (sundhedsdata / henvisning)

Persondata politik (kunder)

I forbindelse med behandlinger her på klinikken er det nødvendigt, at FDHI noterer og behandler oplysninger om patienten.

Hvilke oplysninger behandler FDHI?

I forbindelse med behandling på klinikken noterer FDHI oplysninger om patientens helbredsmæssige forhold til brug for den journalførelse, som FDHI efter sundhedslovgivningen har pligt til at foretage. De nærmere regler findes i autorisationslovens kapitel 6 og journalbekendtgørelsen (bkg. nr. 1090 af 28. juli 2016 om 1090 om autoriserede sundhedspersoners patientjournaler).

Udover de helbredsoplysninger FDHI selv noterer om patienten, kan FDHI modtage helbredsoplysninger om patienten fra andre sundhedspersoner, f.eks. Privatpraktiserende læge, efter reglerne i sundhedslovens kapitel 9.

Oplysningerne anvendes til brug for en god og sikker behandling af patienten og de administrative funktioner, der er forbundet hermed. FDHI har pligt til at opbevare patientens oplysninger sikkert og fortroligt.

FDHI kan også registrere andre oplysninger om patienten til brug for afregningsformål. Disse oplysninger noteres med hjemmel i databeskyttelsesforordningens art. 6, stk. 1, litra b og f [indtil 25. maj 2018: persondatalovens § 6, stk. 1, nr. 2 og nr. 7]. FDHI kan også anvende patientens kontaktoplysninger til brug for udsendelse af nyhedsbreve eller andre markedsføringsmæssige tiltag. I så fald indhenter FDHI først patientens samtykke. Denne anvendelse sker med hjemmel i databeskyttelsesforordningens art. 6, stk. 1, litra a [indtil 25. maj 2018: persondatalovens § 6, stk. 1, nr. 1].]

Videregivelse af oplysninger

Efter sundhedsloven har FDHI personale tavshedspligt om patientens helbredsmæssige og andre følsomme forhold, men hvis det er nødvendigt, kan vi udveksle patientens helbredsoplysninger internt blandt vort personale. Videregivelse af helbredsoplysninger uden for klinikken må som udgangspunkt kun ske med patientens samtykke. I særlige tilfælde kan der efter reglerne i sundhedsloven ske videregivelse uden samtykke. Det vil typisk være til andre sundhedspersoner, f.eks. Patientens egen læge. De nærmere regler herom findes i sundhedslovens kapitel 9.

De oplysninger FDHI har registreret til brug for afregningsformål, udveksles med betalingsformidlere i det omfang, det er nødvendigt for at gennemføre betalingerne. Hvis patientens behandling helt eller delvist betales af andre, f.eks. af en region eller af et forsikringsselskab, vil FDHI også videregive oplysninger om behandlingen til den, der skal betale.

Hvor længe opbevares oplysningerne?

En journal opbevares i det tidsrum, der er fastlagt af Styrelsen for Patientsikkerhed. Det gældende tidsrum er 5 år fra det seneste notat i journalen, jf. journalbekendtgørelsens § 15, stk. 2. I særlige tilfælde kan journalen opbevares længere. Oplysninger til brug for afregningsformål opbevares så længe, det er nødvendigt af hensyn til afregning og bogføring.

Patientens rettigheder vedrørende oplysningerne

Patienten kan få indsigt i hvilke oplysninger, FDHI har registeret, ved at kontakte klinikken. Efter autorisationslovens § 24 må vi ikke slette oplysninger i en journal, men hvis patienten mener, at der er fejl i journalen, kan patienten bede om, at der laves en tilføjelse. For oplysninger, der ikke er omfattet af patientjournalen, har patienten har ret til at få rettet eller slettet ukorrekte oplysninger. Patienten har også ret til at bede klinikken om at ophøre med at behandle sådanne oplysninger om patienten.

Klage

Klager over FDHI's behandling af personoplysninger kan indgives til Datatilsynet, Borgergade 28, 5. sal, 1300 København K. Find nærmere oplysninger om Datatilsynet på www.datatilsynet.dk Tilsyn med reglerne i sundhedslovgivningen føres af Styrelsen for Patientsikkerhed. Styrelsens kontaktoplysninger findes på www.stps.dk

Brud på Datasikkerhed

1. Ved brud på persondatasikkerheden anmelder FDHI uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Foretages anmeldelsen til Datatilsynet ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen. http://kammeradvokaten.dk/nyheder/2017/11/nye-retningslinjer-anmeldelse-af-brud-paa-persondatasikkerheden/

2. Anmeldelsen skal mindst:
   2.1. beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
   2.2. angive navn på og kontaktoplysninger på Direktør og indehaver Thomas Höfelsauer eller Lars Bryde Lind hvor yderligere oplysninger kan indhentes
   2.3. beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
   2.4. beskrive de foranstaltninger, som FDHI har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

3. Når og for så vidt som det ikke er muligt at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

4. FDHI dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte Datatilsynet i stand til at kontrollere, at ovenstående er overholdt.

5. Aktiviteter mhp. implementering
   5.1. Nr. 1: Den ansvarlige opretter og fører en log over alle brud på persondatasikkerheden, som konstateres af den ansvarlige for persondatapolitikken, meddeles fra FDHI's medarbejdere eller fra (under-)databehandlerne i alle tilfælde, uanset om der skal ske anmeldelse til Datatilsynet.
   5.2. Nr. 2: Den ansvarlige vurderer ved hvert konstateret brud på persondatasikkerheden, om der skal ske anmeldelse. Ved denne vurdering anvender den ansvarlige flow chart i bilag A, side 32 i "Vejledning om håndtering af brud på persondatasikkerheden": https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf
   5.3. Nr. 3: FDHI anvender så vidt muligt den standardformular til anmeldelse, som fremgår af Datatilsynets hjemmeside, hvis den ansvarlige efter i FDHI konkluderer, at der skal ske anmeldelse. (Link)
   5.4. Vejledning udgivet februar 2018 af Justitsministeriet og Datatilsynet: "Vejledning om håndtering af brud på persondatasikkerheden": https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf

Underretning om brud på persondatasikkerheden til den registrerede.

6. Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter FDHI uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden.

7. Underretningen af den registrerede skal i et klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde følgende oplysninger og foranstaltninger:
   7.1. angive navn på og kontaktoplysninger på den ansvarlige, hvor yderligere oplysninger kan indhentes
   7.2. beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
   7.3. beskrive de foranstaltninger, som FDHI har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
8. Det er ikke nødvendigt at underrette den registrerede, hvis en af følgende betingelser er opfyldt:
   8.1. FDHI har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering
   8.2. FDHI har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel

8.3. det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal FDHI i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

9. Aktiviteter mhp. Implementering
   9.1. Nr. 1: Den ansvarlige opretter og fører en log over alle brud på persondatasikkerheden, som konstateres af den ansvarlige for persondatapolitikken, meddeles fra FDHI's medarbejdere eller fra (under-)databehandlerne i alle tilfælde, uanset om der skal ske anmeldelse til Datatilsynet.
   9.2. Nr. 2: Den ansvarlige vurderer ved hvert konstateret brud på persondatasikkerheden, om der skal ske anmeldelse. Ved denne vurdering anvender den ansvarlige flow chart i bilag A, side 32 i "Vejledning om håndtering af brud på persondatasikkerheden": https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf
   9.3. Nr. 3: FDHI anvender så vidt muligt den standardformular til anmeldelse, som fremgår af Datatilsynets hjemmeside, hvis den ansvarlige efter i FDHI konkluderer, at der skal ske anmeldelse.
   9.4. Vejledning udgivet februar 2018 af Justitsministeriet og Datatilsynet: "Vejledning om håndtering af brud på persondatasikkerheden": https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf

Medarbejdernes overholdelse af persondatapolitikken

10. Instrukser til medarbejdere i at overholde persondatapolitikken
    10.1. sikrer FDHI, at alle ansatte, herunder fastansatte og personer, som midlertidigt arbejder for FDHI (samlet betegnet "medarbejdere"), overholder de relevante retningslinjer i persondatapolitikken.
    10.2. FDHI's medarbejdere, som får adgang til personoplysninger, kun behandler disse efter instruks fra FDHI, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.
    10.3. FDHI's medarbejdere - i forlængelse af ovenstående - kun anvender FDHI's persondata, i det omfang det er krævet for at udføre det arbejde, som medarbejderen udfører for FDHI.
    10.4. FDHIs medarbejdere, der opdager trusler mod eller brud på persondatasikkerheden, pålægges straks at meddele dette til den ansvarlige for efterlevelse af persondatapolitikken.
    10.5. FDHIs medarbejdere, som bryder persondatasikkerheden, efter en konkret vurdering kan udsættes for ansættelsesretlige eller kontraktuelle konsekvenser.
    10.6. FDHI har – i forlængelse af ovenstående - informeret medarbejderne om og har accepteret at overholde de relevante retningslinjer i persondatapolitikken.

11. Aktiviteter mhp. Implementering
    11.1. Nr. 1: Den ansvarlige sikrer, at alle medarbejdere accepterer ovenstående krav ved at sørge for, at ovenstående krav fremgår af eksempelvis ansættelsesaftaler, praktikforløbskontrakter mv.
    11.2. Nr. 2: Den ansvarlige sikrer, at personaleoplysninger sker i overensstemmelse med Datatilsynets vejledning herom: Der kommer en ny vejledning om dette til maj:

”Databeskyttelse på det ansættelsesretlige område”:
https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordninge n/

12. Baggrund:
    12.1. GDPR: Art. 5 (Principperne om behandling af personoplysninger), art. 24 (Passende organisatoriske foranstaltninger), art. 32, stk. 4 (Enhver fysisk person, der udfører arbejde for den dataansvarlige, og som får adgang til personoplysninger, må kun behandle disse efter instruks fra den dataansvarlige)
    12.2. Vejledning udgivet af Datatilsynet (opdateret 6. maj 2015), ”Krav om datasikkerhed i forbindelse med personaleadministration”:
    https://www.datatilsynet.dk/erhverv/personaleadministration/krav-om-datasikkerhe d-i-forbindelse-med-personaleadministration

Udarbejdet af Lars Bryde Lind & Thomas Höfelsauer maj 2018