

Risici forbundet med datalagring					
Emne	Forklaring af emne	Konsekvenser	Relation til SAFE app	Hvad kan du gøre?	Litteratur
Databrud i form af et serverhack eller frakobling af links	Et databrud involverer adgang til eller ødelæggelse, ændring eller frigivelse af personoplysninger i en organisation, uden at dette er den pågældende organisations hensigt. Links for eksempel til film og hjemmesider frakobles.	Der kan ikke ske databrud i form af et serverhack. Appbrugerens e-mailadresse knyttes til personlige data, der allerede findes online for eksempel på din Apple konto eller i app-store. Skuffelse, når link ikke virker.	Der findes ikke datalagring i SAFE appen. SAFE app indeholder ikke personlige data. Appen gennemgås på ugentlig basis med henblik på fejlfinding.	Brugeren vælger selv, hvilken data de vil dele fra eksempelvis <i>Min side</i> . Send en mail om den opdagede fejl til safeapp@regionsjaelland.dk	Autoriteit Persoongegevens. Data breach caused by ransomware. Available at: https://autoriteitpersoonsgegevens.nl/en/themes/security/data-breaches/data-breach-caused-by-ransomware . Accessed 20-12-2024, 2024.
Emne	Forklaring af emne	Konsekvenser	Relation til SAFE app	Hvad kan du gøre?	Litteratur
At bryde fortroligheden	De delte oplysninger er af fortrolig karakter.	SAFE app opretholder det højeste niveau af databeskyttelse for at beskytte brugsdata bedst muligt. Både europæiske og danske standarder overholdes. SAFE opfylder betingelser for databeskyttelse ved ISAE3000 og er kvalitetssikret og godkendt af appbiblioteket Mind apps.	De indsamlede data er ikke kvalificeret som medicinske data. Det er ikke (inter)nationalt anerkendte medicinske data. Brugere kan selv indtaste personlige og medicinske data i noter i appen. SAFE app beder ikke om dette; brugerne vælger selv, om de vil benytte dette værktøj.	Brugere kan vælge ikke at indtaste personlige data i SAFE app.	European Union. Data protection. Available at: https://commission.europa.eu/law/law-topic/data-protection_en Accessed 20-12-2024, 2024
Privatliv i projekt-processen: brug af biometri	Biometrisk autentificering er autentificering via dit fingeraftryk eller ansigtsscanning. Det betyder, at du låser din enhed eller konto op ved at bruge din finger, dit øje eller ansigt.	Brug af teknologi kan rejse spørgsmål eller modstand. Ved brug af SAFE app, kan der opstå tvivl om datalagring i appen.	For at bruge SAFE app skal brugeren forinden have logget ind på sin egen telefon. Dette kan ske med biometri eller med PIN-kode.	For at bruge SAFE app skal brugeren være logget ind på mobilen. SAFE app kræver ikke yderligere selvstændigt login.	
Anvendte data: sårbare grupper	SAFE app er udviklet af brugere og deres netværk (familie, venner og sundhedsprofessionelle), og er	Sårbare mennesker, pårørende og fagprofessionelle kan bruge appen.	SAFE app er særligt tilegnet sårbare grupper, da appen anvender lægmands sprog og er udviklet af brugere.	Hvis du oplever, at SAFE app har stødende sprogbrug, kontakt da venligst: safeapp@regionsjaelland.dk	Arsenijevic, J., Tummers, L. & Bosma, N. Adherence to electronic health tools among vulnerable groups: Systematic literature review and meta-

	<p>derfor særligt anvendelig til mennesker med levede erfaringer og sårbare grupper.</p> <p>E-sundhedsværktøjer er ikke udbredt brugt blandt udsatte grupper.</p> <p>Overholdelsesraterne er generelt lave, hvilket indikerer, at mange brugere ikke konsekvent anvender disse værktøjer.</p>	<p>Værktøjer, der inkorporerer multimodalt indhold (som videoer) og giver mulighed for direkte kommunikation med sundhedsudbydere, gør værktøjerne mere tilgængelige og brugervenlige.</p>	<p>I SAFE app findes inkorporerede multimodalt indhold i form af eksempelvis Ball stick behandlingsvideoer og meditationsvideoer.</p>	<p>Brug værktøjerne med omtanke og skriv gerne til overstående e-mail, hvis du har ideer til tilpasning af denne digitale sundhedsteknologi.</p>	<p>analysis. Journal of Medical Internet research. 2020;22(2):e11613 doi:10.2196/11613</p>
--	---	--	---	--	--