Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:
Direktoratet for e-helse

Informasjonssikkerhet ved utførelse av testing

Støttedokument
Faktaark nr. 48
Versjon: 1.2
Dato: 01.10.2018

Formål	Sikre at den som utfører testing har tilstrekkelig kunnskap til å sikre konfidensialitet, integritet, tilgjengelighet og kvalitet.		
Ansvar	Virksomhetens leder som skal påse at informasjonssikkerheten er ivaretatt ved utførelse av tester. Det daglige ansvaret for å påse dette i praksis, kan delegeres til for eksempel IKT-ansvarlig og avdelingsleder hvor testen gjennomføres.		
Gjennomføring	Før og under utførelse av testing.		
Omfang	All testing av systemer som inngår i behandling av helse- og personopplysninger.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder / sikkerhetskoordinator ☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☒ Medarbeider/ansatt ☐ Databehandler ☐ Personvernombud
Hjemmel	Personvernforordningen artikkel 32 Pasientjournalloven § 22 Helseregisterloven § 21		
Referanser	• Norm for informasjonssikkerhet • Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet • Faktaark 43 – Bruk av testdata i systemer som inneholder helse- og personopplysninger • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf		

Merknad 01.10.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Med "***testansvarlig***" menes den som er ansvarlig for at testen gjennomføres.

Med "***testbruker***" menes den som operativt utfører testen (enten ansatt hos dataansvarlig eller hos leverandør/databehandler).

Tilrettelegging av testdata følger av Faktaark 43 - Bruk av testdata i systemer som inneholder helse- og personopplysninger.

Nr	Handling
1.	**Prosedyre for utførelse av testing** a) Testansvarlig skal utarbeide en prosedyre som minimum skal omfatte punktene nedenfor i dette faktaarket
2.	**Taushetsplikt** a) Testansvarlig skal føre oversikt over hvem som deltar i testen og at taushetsplikten er ivaretatt b) Testbruker skal på eget initiativ påse at taushetsplikten er formalisert enten ved ansettelsesavtale eller ved særskilt skjema som signeres før oppstart av testen
3.	**Egen testrolle med brukernavn og passord** a) Den enkelte testbruker skal tildeles en egen personlig rolle med brukernavn og passord og ikke benytte sin ordinære autorisasjon

Nr	Handling
	b) I hendelsesregistre skal testbrukeren registreres med egen rolle for testing slik at det ved analyse av hendelsesregistre ikke fremstår som om testbrukeren har utført ulovlige handlinger (jfr helseregisterloven § 13 a og helsepersonelloven § 21 a).
4.	**Nivå 4 for autentisering ved ekstern tilgang** a) Testbruker skal benytte Nivå 4 for autentisering fra hjemmekontor for tilgang til helse- og personopplysninger som inngår i testing (jfr Faktaark 29 – Hjemmekontor og Faktaark 36 Fjernaksess for vedlikehold og oppdateringer)
5.	**Sikring av bærbart utstyr** a) Bruk av bærbart utstyr skal følge kravene til sikring fastsatt i Faktaark 18 – Sikring av bærbart utstyr hvor to av hovedkravene er kryptering av lagringsmedia iht gjeldende krav og sikkerhetsnivå 4 ved tilgang til helse- og personopplysninger
6.	**Sikring av trådløst nettverk** a) Bruk av trådløst nettverk skal følge kravene til sikring fastsatt i Faktaark 26 – Sikring av trådløs teknologi hvor et av hovedkravene er kryptering av datakommunikasjonen b) Kravet gjelder bruk av trådløst nettverk på arbeidsplass og ved hjemmekontor (jfr Faktaark 29 – Hjemmekontor)
7.	**Oppbevaring av utskrifter** a) Testbruker skal låse inn utskrifter som inneholder helse- og personopplysninger b) Dette kan gjøres ved å låse kontoret eller låse inn utskrifter i egen skuff eller skap
8.	**Makulering av utskrifter** a) Testansvarlig skal orientere om hvor makuleringsutstyr finnes og hvordan det brukes b) Testbruker skal makulere utskrifter etter at formålet med utskriften er oppnådd
9.	**Sikring av minnepinne, CD og andre flyttbare lagringsmedier (omtalt som minnepinne)** a) Minnepinne som benyttes til lagring av testdata, filer som inneholder helse- og personopplysninger, osv skal ikke flyttes ut fra egen arbeidsplass b) Minnepinne skal oppbevares som utskrifter c) Minnepinne med kryptering iht gjeldende krav kan bringes ut fra arbeidsplassen d) Minnepinne som ikke er kryptert skal slettes med godkjent sletteløsning (jfr Faktaark 34 – Håndtering av lagringsmedia) **c)** Minnepinne som inneholder helse- og personopplysninger skal merkes
10.	**Sikring av fysisk område testingen utføres i (kontor, hjemme)** a) Ved testing utenfor egen arbeidsplass skal reglene for hjemmekontor ivaretas (jfr Faktaark 29 – Hjemmekontor)
11.	**Bruk av e-post** a) E-post skal ikke benyttes til sending av helse- og personopplysninger
12.	**Beskrivelse av feil og mangler** a) Feil og mangler skal som hovedregel ikke beskrives med identifiserbare helse- og personopplysninger b) Beskrives feil og mangler med identifiserbare helse- og personopplysninger skal datafiler sikres som helse- og personopplysninger og utskrifter som beskrevet ovenfor
13.	**Avviksrapportering** a) Alle avvik fra etablerte prosedyrer skal rapporteres som avvik iht prosedyre for avviksbehandling (jfr Faktaark 8 – Avviksbehandling)