Sikkerhetsrevisjon iflg. faktaark nr. 6 fra Norm for informasjonssikkerhet

Nr	Sjekkpunkt	Faktaark	Ok/ikke ok	Beskrivelse
1	Er det gjennomført nødvendig(e) risikovurdering(er) siste år?	7	Ikke ok	Er gjennomført en rekke ROS-analyser vedr. FIKS. Det mangler i vesentlig grad risikovurderinger innen de områder som HNIKT har ansvaret for. HNIKT burde snarest iverksette ROS analyser.
2	Er prosedyrene for avviksbehandling ift. informasjonssikkerhet kjent i virksomheten?	8	Ok	29 meldte info.sikk.avvik i 2014. En økning fra 17 i 2013.
3	Fungerer avviksbehandling ift. informasjonssikkerhet?	8	Ikke ok	De ansatte har nok fortsatt en noe for høy terskel før de melder informasjonssikkerhets avvik, de fleste gjelder fortsatt pasientopplysninger funnet i tøy.
4	Er det etablert nødprosedyrer ved stans i informasjonssystemene?	11 HN-IKT	Ok	Nødprosedyrer for DIPS er etablert. Fra teknisk side (HN-IKT) foreligger det rutiner for håndtering av krisesituasjoner, i tillegg til vaktordninger 24/7. Ved linjebrudd har vi også nå redundante linjer (doble linjer)
5	Gjennomføres det jevnlig kontroll/gjennomgang av hendelsesregistre?	15	Ikke ok	Gjennomføres 4 innsynskontroller årlig, ingen funn av alvorlig karakter. Blåslyslogg gennomføres månedlig. Ved mistanke/behov kan det også bli gjennomført kontroll. Oppfølging av innsynskontrollene har ikke vært gjort i god nok grad.
6	Krypteres helse- og personopplysninger (f.eks. meldingsformidling) som overføres i åpne nett?	16 og 24 HN-IKT	OK	Når det gjelder den delen som faller under Faktaark 24, så krypteres all trafikk mellom sykehusene på nettverksnivå.
7	Er det etablert tilfredsstillende fysisk sikring av områder og datautstyr?	17 HN-IKT	Ok	Dette er i varierende grad tilfredstillende utenom server rom. De største installasjone er i samsvar med PR05786 ”Fysisk sikring”. Nytt midl. datasenter i Tromsø er oppe og går og ROS-analyser er gjennomført her.
8	Er lagringsenhet på bærbart utstyr som benyttes til helse- og personopplysinger kryptert?	18 HN-IKT	Ok	Etter gjeldende prosedyrer er ikke personopplysninger tilgjengelig for lagring på bærbart utstyr. Bærbare datamaskiner som brukes ute på Internett, er gjennom konfigurering ikke godkjent for tilkopling inn på lokalnett for direkte

				tilgang til tjenester med sensitive personopplysninger.
Nr	**Sjekkpunkt**	**Faktaark**	**Ok/ikke ok**	**Beskrivelse**
9	Oppdateres antivirusprogramvaren kontinuerlig?	19 HN-IKT	Ok	Ja, antivirusprogramvaren oppdateres hver time. HN IKT jobber fortløpende med å sikre utstyr som de er ansvarlig for.
10	Tas det daglig sikkerhetskopi?	21 HN-IKT	Ikke ok	Ja, backup tas på alle 3 sykehus enhetene. Men har det vært gjennomført tilbakelegging av backup?
11	Oppbevares sikkerhetskopier utenfor huset?	21 HN-IKT	Ok	Ja. Sykehusene har Gb samband og backup skjer til Bodø eller Tromsø der de har backup roboter. Alt av backup går dit. HN-IKT har i driftsavtale med oss ansvar for backup.
12	Er det kontroll med all ekstern tilgang til datasystemer?	22 HN-IKT	Ok	Ekstern tilgang skal være i samsvar med etablerte prosedyrer.
13	Følges ”Veileder for fjernaksess for vedlikehold og oppdateringer mellom leverandør og helsevirksomhet” ved eventuell ekstern tilgang?	36 HN-IKT	Ok	Samme svar som til pkt.12
14	Er det etablert relevante avtaler for forskningsprosjekter?	23	Ok	Ja
15	Slettes helse- og personopplysinger når formålet med behandlingen er avsluttet?	25 HN-IKT	Ok	Vedr. Pasopp undersøkelsene blir alt slettet når det skal, her må dedikerte HN-IKT personell svare på om det er gjort.
16	Brukes trådløst utstyr og nett iht. etablerte prosedyrer?	26 HN-IKT	Ikke ok	Sandnessjøen benytter eget oppsatt trådløst nett til telemetri.
17	Etterleves prosedyrene for makulering?	27	Ikke ok	I og med at det registreres avvik der pasientsensitiv informasjon finnes i klær, etterleves det ikke 100%.
18	Etterleves prosedyrene for bruk av e-post og Internett?	27 og 33	Ikke ok	Alle ansatte er nok kjent med at man ikke skal sende pasientinformasjon på e-post, men vi har ikke kontroll på om det faktisk skjer. Gjestepas. data overføres bl.a på e-post.
19	Etterleves prosedyrene for hjemmekontor og mobilt utstyr?	29 og 30 HN-IKT	Ikke ok	Er usikre på om alt utstyr som brukes er korrekt satt opp og om all bruk er iflg. våre prosedyrer

Nr	Sjekkpunkt	Faktaark	Ok/ikke ok	Beskrivelse
20	Er det etablert løsning og prosedyrer for autentisering på sikkerhetsnivå 4 ved bruk av mobiltelefoner og nettbrett for tilgang til helseopplysninger?	30 HN-IKT	Ok	Ikke relevant da det pt ikke er etablert løsninger for tilgang til personopplysninger fra mobiltelefoner og nettbrett
21	Byttes passord iht. prosedyrene?	31	OK	Ja. Synkronisering av brukernavn/passord fra flere systemer er allerede etablert og flere vil komme i 2015.
22	Følges veileder ”Personvern og informasjonssikkerhet i forskningsprosjekter innefor helse- og omsorgssektoren” ifm utlevering av helse- og personopplysninger?	40	Ok	I de aktuelle forskningsprosjektene gjøres det.
23	Etterleves reglene for bruk av SMS i pasientkontakt?	42	Ikke ok	Er ikke implementert SMS løsning i DIPS. Hva avdelingene evt. sender ut sjøl har vi ikke kontroll med.
24	Etterleves reglene for bruk av testdata i systemer som inneholder helse- og personopplysninger?	43 HN-IKT	Ok	Er ikke kjent med at det ikke etterleves.

Pkt.'er som ikke er ok:

Nr	Sjekkpunkt	Faktaark	Ok/ikke ok	Beskrivelse
1	Er det gjennomført nødvendig(e) risikovurdering(er) siste år?	7	Ikke ok	Er gjennomført en rekke ROS-analyser vedr. FIKS, men innenfor andre områder burde HN-IKT også ha gjennomført
3	Fungerer avviksbehandling ift. informasjonssikkerhet?	8	Ikke ok	De ansatte har nok fortsatt en noe for høy terskel før de melder informasjonssikkerhets avvik, de fleste gjelder fortsatt pasientopplysninger funnet i tøy.
5	Gjennomføres det jevnlig kontroll/gjennomgang av hendelsesregistre?	15	Ikke ok	Gjennomføres 4 innsynskontroller årlig, ingen funn av alvorlig karakter. Blåslyslogg gennomføres månedlig. Ved mistanke/behov kan det også bli gjennomført kontroll. Oppfølging av innsynskontrollene har ikke vært gjort i god nok grad.
10	Tas det daglig sikkerhetskopi?	21 HN-IKT	Ikke ok	Ja, backup tas på alle 3 sykehus enhetene. Men har det vært gjennomført tilbakelegging av backup?
16	Brukes trådløst utstyr og nett iht. etablerte prosedyrer?	26 HN-IKT	Ikke ok	Sandnessjøen benytter eget oppsatt trådløst nett til telemetri.
17	Etterleves prosedyrene for makulering?	27	Ikke ok	I og med at det registreres avvik der pasientsensitiv informasjon finnes i klær, etterleves det ikke 100%.
18	Etterleves prosedyrene for bruk av e-post og Internett?	27 og 33	Ikke ok	Alle ansatte er nok kjent med at man ikke skal sende pasientinformasjon på e-post, men vi har ikke kontroll på om det faktisk skjer. Gjestepas. data overføres bl.a på e-post.
19	Etterleves prosedyrene for hjemmekontor og mobilt utstyr?	29 og 30 HN-IKT	Ikke ok	Er usikre på om alt utstyr som brukes er korrekt satt opp og om all bruk er iflg. våre prosedyrer
23	Etterleves reglene for bruk av SMS i pasientkontakt?	42	Ikke ok	Er ikke implementert SMS løsning i DIPS. Hva avdelingene evt. sender ut sjøl har vi ikke kontroll med.

Tiltak:

Punkt	Innhold	Tiltak
1	Er det gjennomført nødvendig(e) risikovurdering(er) siste år?	Be om en redegjørelse fra HN-IKT på gjennomførte ROS-analyser vedr. deres drift av Helgelandssykehuset.
3	Fungerer avviksbehandling ift. informasjonssikkerhet?	Tiltak nødvendig for å få de ansatte til å melde flere typer info.sikk avvik. Forslag fra Fagstab utarbeides.
5	Gjennomføres det jevnlig kontroll/gjennomgang av hendelsesregistre?	Oppfølging av innsynskontrollene gjennomføres.
10	Tas det daglig sikkerhetskopi?	Ønsker oversikt fra HN-IKT at test av tilbakelegging av backup er gjennomført.
16	Brukes trådløst utstyr og nett iht. etablerte prosedyrer?	Sandnessjøen benytter eget oppsatt trådløst nett til telemetri. Dette må verifiseres. En gjennomgang ved alle enhetene må gjennomføres.
17	Etterleves prosedyrene for makulering?	I og med at det registreres avvik der pasientsensitiv informasjon finnes i klær, etterleves det ikke 100%. Tiltak og informasjon må iverksettes.
18	Etterleves prosedyrene for bruk av e-post og Internett?	Alle ansatte er nok kjent med at man ikke skal sende pasientinformasjon på e-post, men vi har ikke kontroll på om det faktisk skjer. Gjestepas. data overføres bl.a på e-post. Tiltak og informasjon må iverksettes. Digipost kan benyttes dersom sensitiv informasjon må sendes via e-post.
19	Etterleves prosedyrene for hjemmekontor og mobilt utstyr?	Utstyr som benyttes må gjennomgås og dokumenteres samt hvilke muligheter ansatte har selv til å omgå egne bestemmelser for bruk av utstyr. Oversikt lages.
23	Etterleves reglene for bruk av SMS i pasientkontakt?	Er ikke implementert SMS løsning i DIPS. Hva avdelingene evt. sender ut sjøl har vi ikke kontroll med. Her må en gjennomgang ved alle enhetene gjennomføres. Oversikt lages.

Tiltakene iverksettes.

Dato: 07.04.2015
Sign: adm. direktør

_____