

Hvilke risikoer er vurdert?

Sikkerhet

- 1: Risiko for uautorisert tilgang til personopplysninger som følge av mangelfull fysisk adgangskontroll
- 2: Risiko for uautorisert tilgang til personopplysninger som følge av mangelfulle prosedyrer for dokumenthåndtering
- 3: Risiko for uautorisert tilgang til personopplysninger som følge av mangelfull kontroll av systemtilgang
- 4: Risiko for uautorisert tilgang til personopplysninger som følge av mangelfulle prosedyrer for tilgangsstyring
- 5: Risiko for feil bruk av systemene som følge av manglende kunnskap om bruk av systemet

Bruk av og kunnskap om personopplysninger

- 6: Risiko for uautorisert tilgang til personopplysninger som følge av fysisk lagring utenfor PRO og NISSY
- 7: Risiko for uautorisert tilgang til personopplysninger som følge av lagring i elektroniske system utenfor PRO og NISSY
- 8: Risiko for feil i saksbehandling som følge av utdatert/feilaktig informasjon i lokale systemer
- 9: Risiko for brudd på regelverk (lov, forskrift avtale) som følge av sammenstilling av informasjon mellom PRO/NISSY og andre systemer
- 10: Risiko for personopplysninger på avveie som følge av at personopplysninger blir utlevert til feil eller uautoriserte personer
- 11: Risiko for personopplysninger på avveie som følge av bruk av ukryptert e-post

- 12: Risiko for brudd på regelverk (lov, forskrift avtale) som følge av manglende kunnskap internt
- 13: Risiko for brudd på regelverk (lov, forskrift avtale) som følge av manglende kunnskap hos rekvirenter

Eksterne avtaleparter

- 14: Risiko for feil håndtering av personopplysninger som følge av manglende/mangelfull **avtale** med underleverandør og deres eventuelle underleverandør(er)
- 15: Risiko for feil håndtering av personopplysninger som følge av manglende/mangelfull **oppfølging** av underleverandør og deres eventuelle underleverandør(er)
- 16: Risiko for feil håndtering av personopplysninger som følge av manglende/mangelfull **opplæring** av underleverandør og deres eventuelle underleverandør(er)

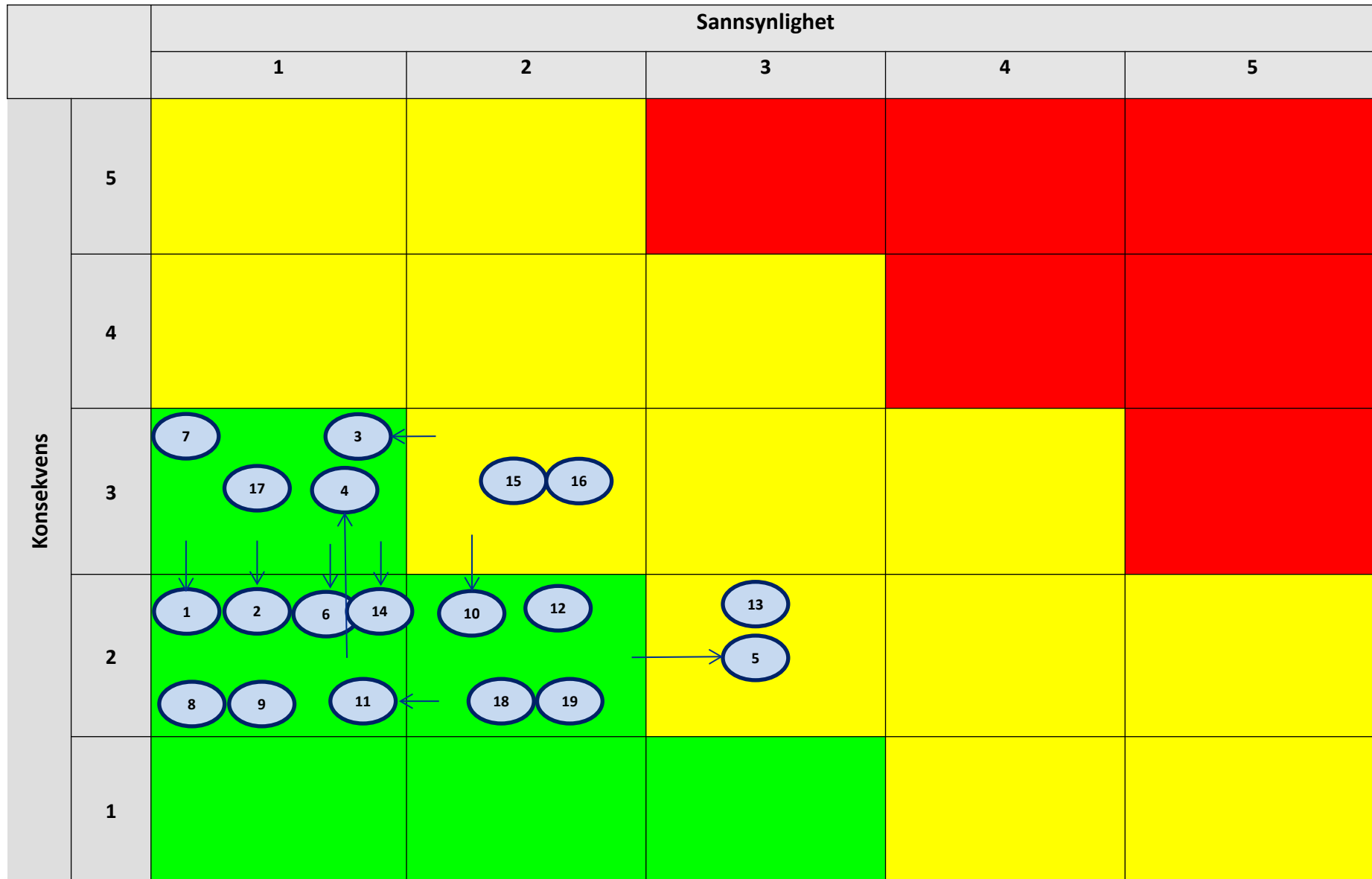
Økonomiske misligheter

- 17: Risiko for økonomiske misligheter som følge av misbruk på saksbehandlernivå
- 18: Risiko for økonomiske misligheter som følge av misbruk på rekvirentnivå

Annet

- 19: Risiko for ukorrekt saksbehandling og utbetaling som følge av utilstrekkelige kontrolltiltak

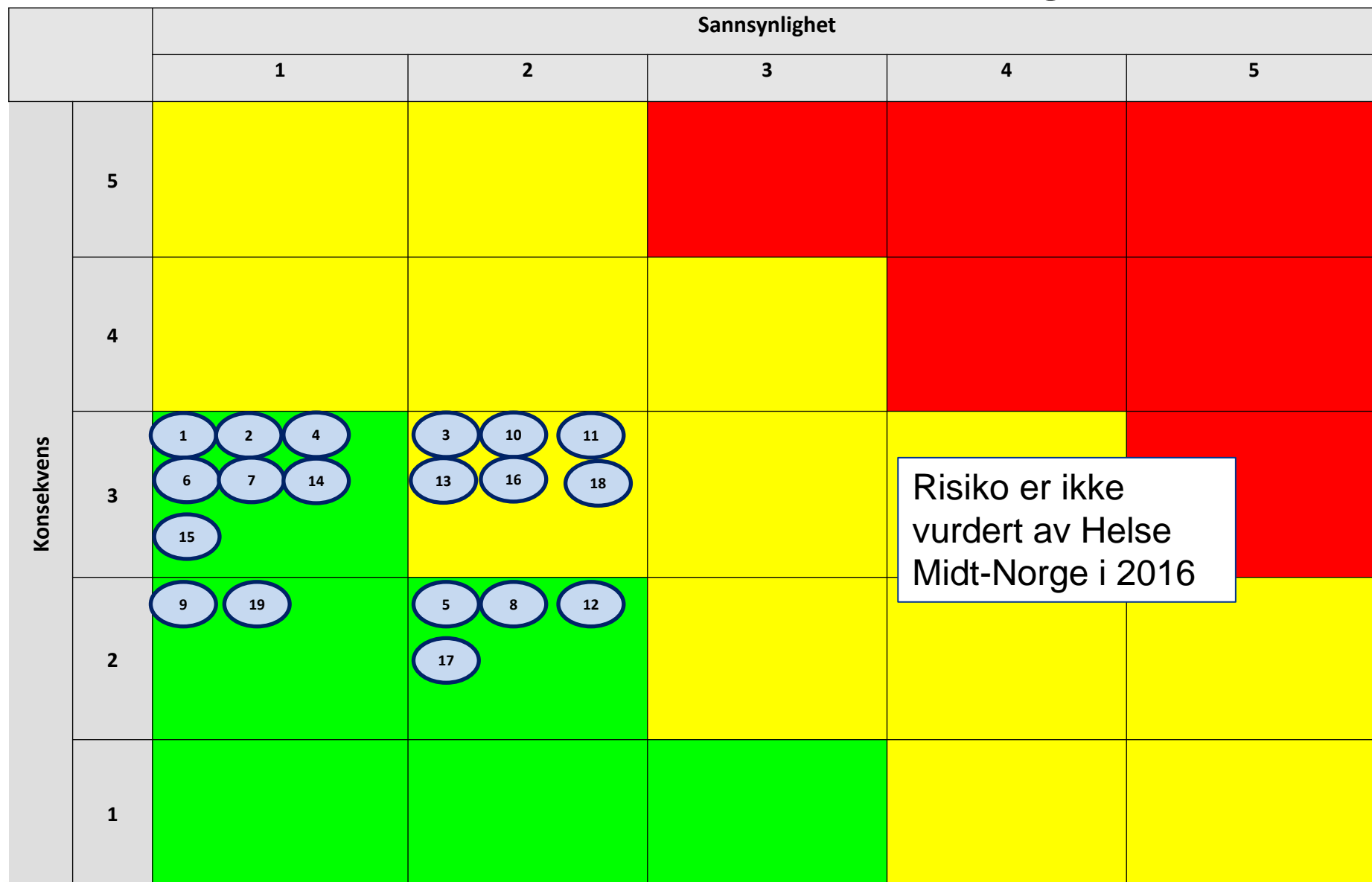
Samlet risikobilde av pasientreiseområdet 2016



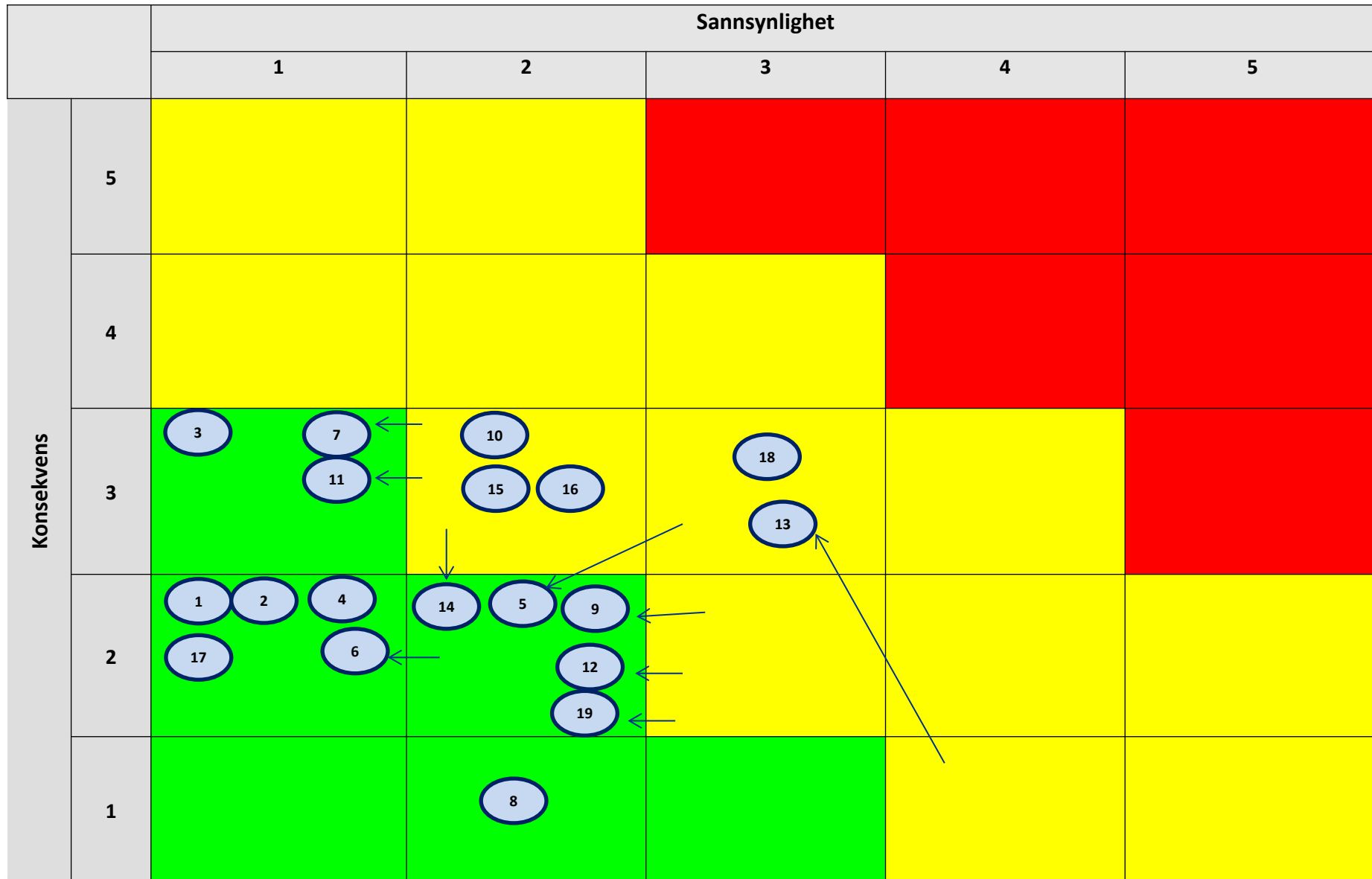
Risikobilde vurdert av PRK i Helse Nord 2016

| | | Sannsynlighet | | | | |
|------------|---|---------------|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Konsekvens | 5 | | | | | |
| | 4 | | | | | |
| | 3 | | | | | |
| | 2 | | | | | |
| | 1 | | | | | |

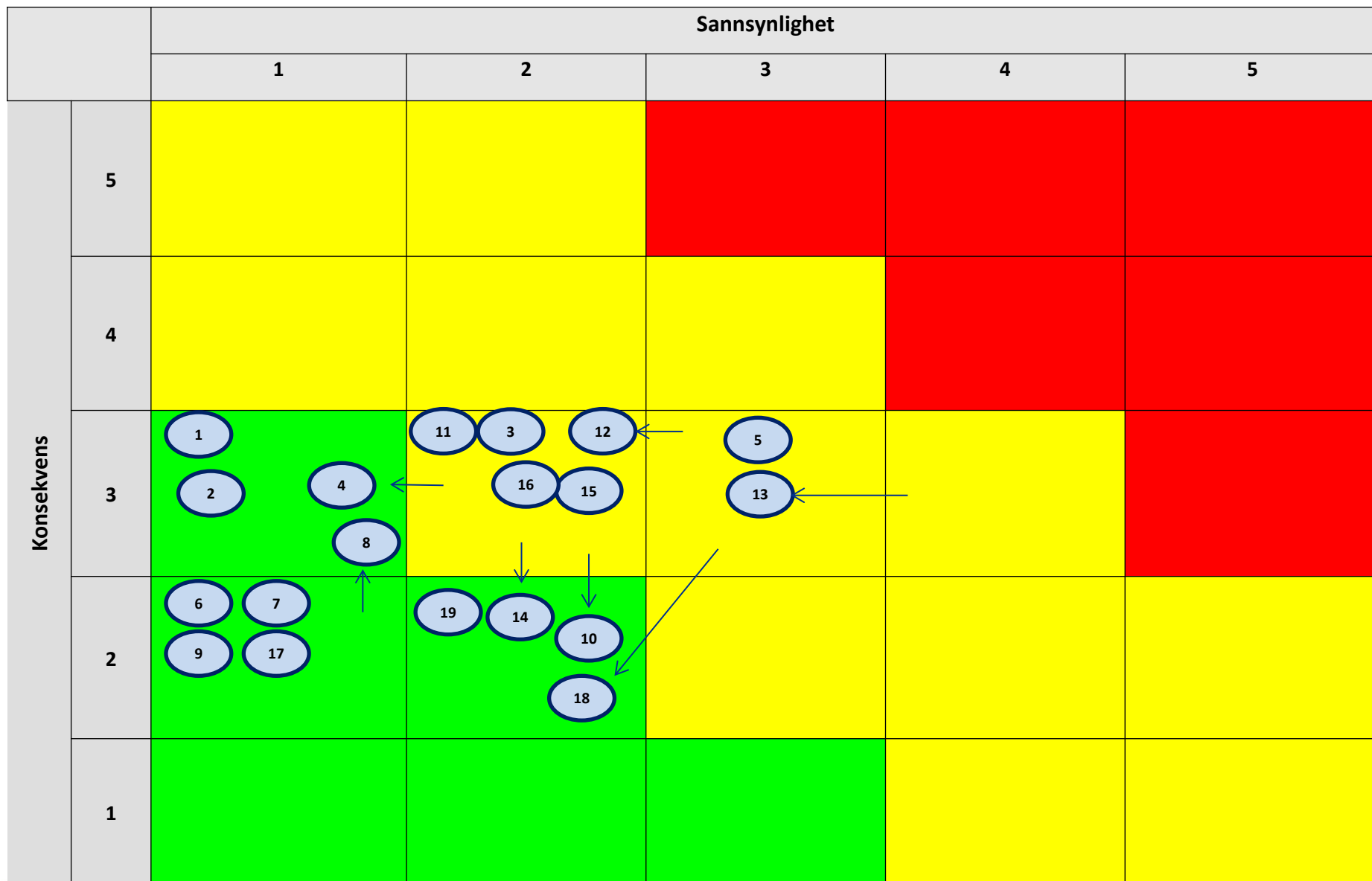
Risikobilde vurdert av PRK i Helse Midt-Norge 2015



Risikobilde vurdert av PRK i Helse Vest 2016



Risikobilde vurdert av PRK i Helse Sør-Øst 2016



Risikobilde vurdert av Pasientreiser ANS 2016

| | | Sannsynlighet | | | | |
|------------|---|---------------|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Konsekvens | 5 | | | | | |
| | 4 | | | | | |
| | 3 | | | | | |
| | 2 | | | | | |
| | 1 | | | | | |

| | | 1 | 2 | 3 | 4 | 5 |
|------------|---|---|--|---|---|---|
| Konsekvens | 5 | | | | | |
| | 4 | | | | | |
| | 3 | <div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">1</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">2</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">6</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">14</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">15</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">17</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">3</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">4</div> </div> | | | | |
| | 2 | <div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">8</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">9</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">11</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">18</div> </div> | <div style="display: flex; flex-wrap: wrap; gap: 5px;"> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">10</div> <div style="border: 1px solid black; border-radius: 50%; padding: 2px 5px;">19</div> </div> | | | |
| | 1 | | | | | |



| | Risikopunkt | S | K | Risiko | Risikoreducerende tiltak | Ansvar | Frister | |
|------------------|--|---|---|--------|---|---|---|--|
| Sikkerhet | | | | | | | | |
| 5 | Risiko for feil bruk av systemene som følge av manglende kunnskap om bruk av systemet (for eksempel at saksbehandler/rekvirent skriver personopplysninger i feil felt) | 3 | 2 | | <p>Gjennomførte tiltak: Kontinuerlig opplæring, oppfølging og informasjon til rekvirenter.</p> <p>Opplæring fra Pasientreiser ANS om håndtering av personopplysninger vinter 2015</p> <p>Skriftlig rutine for bruk av fritekstfelt</p> <p>Ser over tilnærmet alle turer som inneholder merknad til transportør, og sletter eventuelle sensitive opplysninger.</p> <p>Avviksfører og følger opp behandlere som legger inn sensitive opplysninger i merknadsfelt</p> <p>Opplæring og prosedyrer for å sikre riktig håndtering av personopplysninger og bruk av systemene</p> <p>Eget e-læringskurs om personvern</p> <p>Eget e-læringskurs om e-rekvirering (lovverk og praktisk veileder)</p> | <p>Nye tiltak: Systematisk bruk av rapporter fra Radar og avvik som grunnlag for videre oppfølging</p> <p>Ha dialog med PRK for å avklare bruk og informere om riktig praksis.</p> <p>Oppdatere brukerdokumentasjon PRO 3.0</p> <p>«Mine Pasientreiser» standardiserer kommunikasjon og reduserer sannsynligheten for feil input</p> | <p>PRK</p> <p>ANS</p> <p>ANS</p> <p>ANS</p> | <p>Fortløpende</p> <p>15.10.16</p> <p>15.10.16</p> <p>01.10.16</p> |

| | Risikopunkt | S | K | Risiko | Risikoreduserende tiltak | Ansvar | Frister | |
|--|---|---|---|--------|---|---|-----------------------|------------------------------------|
| Bruk av og kunnskap om personopplysninger | | | | | | | | |
| 13 | Risiko for brudd på regelverk (lov, forskrift avtale) som følge av manglende kunnskap hos rekvirenter | 3 | 2 | | <p>Gjennomførte tiltak:</p> <p>Kontinuerlig opplæring av rekvirenter i alle kommuner og alle avdelinger i helseforetaket.</p> <p>Jevnlige samarbeidsmøter med transportører</p> <p>Kontinuerlig og tett oppfølging av rekvirenter som gjør feil (bruk av RADAR som informasjonsgrunnlag).</p> <p>Redigering av rekvisisjoner i NISSY før sending til transportør.</p> <p>E-læringskurs om e-rekvirering (lovverk og praktisk veileder) – dette er et krav ved noen PRK</p> <p>Fokus på lovverket i dialog med rekvirentene</p> | <p>Nye tiltak:</p> <p>Fortløpende dialog og opplæring av rekvirenter gjennom oppfølging av registrerte avvik</p> <p>I samsvar med strategiplan 3.1.3, skal det vurderes konkrete tiltak mot rekvirentledet</p> | <p>PRK</p> <p>ANS</p> | <p>Fortløpende</p> <p>31.12.17</p> |

| | Risikopunkt | S | K | Risiko | Risikoreducerende tiltak | Ansvar | Frister | |
|------------------------------|---|---|---|--------|---|--|-----------------------|---------------------------------------|
| Eksterne avtaleparter | | | | | | | | |
| 15 | Risiko for feil håndtering av personopplysninger som følge av manglende/mangelfull oppfølging av underleverandør og deres eventuelle underleverandør(er) | 2 | 3 | | <p>Gjennomførte tiltak: Noen PRK har i sin avtale at alle leverandører og deres underleverandører skal ha gjennomført e-læringskurs for transportører.</p> <p>Jevnlig gjennomgang av databehandleravtalene mellom pasientreisekontorene og Pasientreiser ANS</p> <p>Gjennomgang av effekt av oppfølging av tiltakene etter revisjonen av tverrgående prosessene (1/2013)</p> | <p>Nye tiltak: Fortsatt gjennomgang av veileder for sjåførere</p> <p>Utforme utkast til standardkrav (eksempelvis miljø, personvenn og e-læring) som kan tas inn i oppdaterte databehandleravtaler og benyttes på andre områder ved behov og ønsker fra det enkelte helseforetak.</p> | <p>PRK</p> <p>ANS</p> | <p>Fortløpende</p> <p>31.12.16</p> |
| 16 | Risiko for feil håndtering av personopplysninger som følge av manglende/mangelfull opplæring av underleverandør og deres eventuelle underleverandør(er) | 2 | 3 | | <p>Gjennomførte tiltak: Noen PRK har avtalt at alle leverandører og deres underleverandører skal ha gjennomført eLæringskurs for transportører.</p> <p>Løpende oppfølging av avvik.</p> <p>Dialogmøte med leverandør. Nytt e-læringskurs om e-rekvirering (lovverk og praktisk veileder)</p> <p>Nasjonalt kartlegging og oppfølging av bruk av personopplysninger i direkte- og enkeltoppgjørsregisteret</p> | <p>Nye tiltak: Fortsatt fokus på lovverket i dialog med rekvirentene</p> <p>Fortløpende vurdering av nye tiltak for å redusere muligheten til å legge inn personopplysninger i direkte- og /enkeltoppgjørregisteret</p> | <p>PRK</p> <p>ANS</p> | <p>Fortløpende</p> <p>Fortløpende</p> |

Oppfølging

- Tiltak og oppfølging av risikoene skal skje i linjen iht ansvar. Eksempelvis må det enkelte foretak følge opp egne risikoer i rødt og gult selv om det akkumulerte er i grønt.
- Områder i rødt krever strakstiltak og skal prioriteres.
- For områder i gult bør det iverksettes tiltak med plan for oppfølging.
- Områder i grønt ansees som godt ivaretatt og krever ikke ytterligere tiltak.