##### The appendix is up to date with version 6.0 of the Code.

##### The requirement table is structured in accordance with the table below and is in accordance with the Code’s table of contents.

| Area | Sub-area |
| --- | --- |
| A. Management and responsibility | 1. Roles and responsibilities regarding information security and data protection
2. The controller’s responsibilities
3. The processor’s responsibilities
4. The management system
5. The management’s review
 |
| B. Risk management | 1. Proportionality in connection with the selection of measures
2. Minimum requirements for safeguarding confidentiality, integrity, availability and robustness
3. Overview of technology and the processing of personal health data
4. Risk assessment and risk management
5. Assessment of data protection consequences
 |
| C. Fundamental considerations regarding the processing of personal health data | 1. Basis for processing
2. Duties and requirements in connection with the processing of personal health data
3. Built-in data protection
 |
| D.Information security | 1. Employees, competence and awareness-raising work
2. Access control
3. Physical security and the handling of equipment
4. Secure IT operation
5. Communication security
6. Digital communication to data subjects
7. Suppliers and agreements
8. Handling of information security breaches
9. Emergency procedures
 |

##### Using the requirement table

##### Amongst other things, the Code requires security audits to be conducted based on an approved plan for security audits. An audit plan may for example be to audit areas A - D above with regard to the questions below on a rolling basis every four years.

##### Explanation regarding the contents of the requirement table below:

**Requirement**

##### The requirement table contains requirements with "shall" in the Code, to make it easy to verify whether the organisation is following the Code. All questions must be answered with “Yes” in order for the requirement to be met. It is recommended that the requirement table be used together with the Code, so that the requirement is assessed in relation to the topic that is considered in the Code.

The organisation shall assess which requirements in the Code apply based on the specific processing of personal data (see section 3.1 of the Code)

**Section in the Code**

##### Reference to section number in the Code.

**Section in ISO 27001**

Reference to section number in ISO 27001 – 2017 and ISO 27001 – 2017 Annex A.

Specially regarding A.18.1: Annex A: indicates that "all relevant statutory, regulatory and contractual requirements and the organizations approach to meeting these requirements shall be explicitly identifies and documented", but without specifying these requirements. This requirement in ISO is not included in the list. It is automatically triggered if the requirement in the Code is based on law/regulation. )If a organization considers to comply with A.18.1, it should be verified that the specific requirements of the Code, are complied with.

\*= The requirement in the Code is partially covered by ISO 27001. The requirement of the Code are more specific and detailed than the requirements of ISO 27001. In these cases, this is marked with a \* behind the chapter number.

(A.X.X\* & A.Y.Y\*) = A.X.X and A.Y.Y is each partially covered by the requirements of the Code. These two requirements are considered together to be in compliance with the relevant requirement in the Code, which is made visible by the use of brackets and the separator "&".

**System requirements in personal health data filing systems for therapeutic purposes**

Specifies security requirements which must be met by systems which process personal health data (formerly Fact sheet 38). For certain requirements, a more detailed clarification of the requirement is provided which cannot be directly deduced from the Code. These are specified as "*Clarification of the requirement:*".

**The requirement does not apply in its entirety or in part to the organisation (Must be justified)**

##### The Code is based on the principle of proportionate safeguarding. When using the requirement table, the organisation must therefore determine which issues are relevant, and strike a balance in relation to the organisation’s size, nature and the scope of processing of personal health data, patient safety, risks, etc. If the requirement is not applied, the controller must explain why the requirement is deleted.

**Is the requirement fulfilled?**

Insert a cross to indicate whether or not the requirement is fulfilled.

**Legal basis for the requirement in law or regulation**

Where there is a legal or regulatory paragraphs, the paragraph is specified in the column. This does not mean that the legal basis covers the entire processing of data or activites. For example if the paragraph is in the Health records act, and the processing of data or activity does not fall within the scope of the law, this will not be a relevant legal basis. The organization must consider this for itself.

The following acronyms for are used in the table for legal basis:

* EFF: eForvaltningsforskriften (eGovernment Regulation)(<https://lovdata.no/dokument/SF/forskrift/2004-06-25-988>)
* FEP: Forskrift om etablering og gjennomføring av psykisk helsevern, Section 49 (Regulation on establishment and provision of mental healthcare, Section 49) (<https://lovdata.no/dokument/SF/forskrift/2011-12-16-1258>)
* FIKT: Forskrift om IKT-standarder i helse- og omsorgstjenesten (Regulation on ICT standards in the healthcare and care services) (<https://lovdata.no/dokument/SF/forskrift/2015-07-01-853>)
* FLK: Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten (Regulation on management and quality improvement in the healthcare and care services) (<https://lovdata.no/dokument/SF/forskrift/2016-10-28-1250>)
* HFL: Helseforskningsloven (Health Research Act) (<https://lovdata.no/dokument/NL/lov/2008-06-20-44>)
* HPL: Helsepersonelloven (Health Personnel Act) (<https://lovdata.no/dokument/NL/lov/1999-07-02-64>)
* HTL: Helse- og omsorgstjenesteloven (Health and Care Services Act )(<https://lovdata.no/dokument/NL/lov/2011-06-24-30>)
	+ Based on what a management body is, the regulation is considered to only be relevant to certain organisations within the sector (see jusinfo.no: *Pursuant to Section 1, the Public Administration Act applies to “the activity that is carried on by public administration bodies” (public sector activity), unless otherwise stipulated in or pursuant to law. The activity of a public administration body is also covered by the Public Administration Act when the administration does not make decisions and exercise public authority, i.e. when the action is not deemed to be "determinative for rights or obligations" and thus does not constitute the "exercising of public authority". In all its activity, the administration is thus subject to the statutory and non-statutory rules concerning public case administration, even when authority or decision-making competence is not exercised."* and Wikipedia *"In Norway, public administration bodies typically comprise the government, ministries, directorates, county municipalities and municipalities. Municipal councils and county councils are also often included."* )
* HTIL: Helsetilsynsloven (Health Supervision Act) (<https://lovdata.no/dokument/NL/lov/2017-12-15-107>)
* PBL: Pasient- og brukerrettighetsloven (Patient Rights Act) <https://lovdata.no/dokument/NL/lov/1999-07-02-63>)
* PJF: Pasientjournalforskriften (Health Records Regulation) (<https://lovdata.no/dokument/SF/forskrift/2019-03-01-168>)
* PJL: Pasientjournalloven (Health Records Act) (<https://lovdata.no/dokument/NL/lov/2014-06-20-42>)
* POL: Personopplysningsloven (Personal Data Act) <https://lovdata.no/dokument/NL/lov/2018-06-15-38>)
* GDPR: General Data Protection Regulation (GDPR) (<https://lovdata.no/dokument/NL/lov/2018-06-15-38>)

**The requirement is fulfilled by the processor**

This column can be used to indicate whether the requirement is fulfilled by the processor. In the case of requirements that cannot be passed on to the processor, the field is greyed out.

Requirements that both the controller and processor shall fulfil are indicated in green.

**Overall summary of the requirements of the Code**

| No. | Requirement | Section in the Code | Section in ISO 27001 | System requirements in personal health data filing systems for therapeutic purposes | The requirement does not apply in its entirety or in part to the organisation(Must be justified) | Is the requirement fulfilled? | Legal basis for the requirement in law or regulation | The requirement is fulfilled by the processor |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Is the selection of appropriate technical and organisational measures assessed in relation to the organisation’s size, nature and scope of the processing of personal health data, patient safety, risks, etc.? | 1.5 | 6.1.1 8.1  |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 6 |  |
|  | Are the selected measures based on risk assessments? | 1.5 | 6.1.3 8.3  |  |  | [ ] Yes [ ] No | GDPR, Section 32GDPR, Section 35(1)PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Are the selected measures proportionate in relation to the size of the organisation and the scope of processing of personal data? | 1.5 | 6.1\*8.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32GDPR, Section 35(1)PJL, Section 22HRL, Section 21 |  |
|  | Does the organisation’s senior management ensure that the organisation follows applicable requirements regarding information security and data protection? | 2 | 5.1 5.25.3 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21HTL, Section 5-10 first pointGDPR, Article 24FLK, Section 7 |  |
|  | Has the organisation’s chief executive determined a level of acceptable risk? | 23.2 | 6.1.2 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32FLK, Section 5 and 6 | [ ] Yes [ ] No |
|  | Has the organisation’s chief executive established rules regarding risk management? | 2 | 6.1.3 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22PLF, Section 6 | [ ] Yes [ ] No |
|  | Has the organisation’s chief executive ensured effective management and control? | 2 | 6.2 |  |  | [ ] Yes [ ] No | GDPR, Article 24 first paragraphFLK, Sections 3 and 4PLF, Section 7 | [ ] Yes [ ] No |
|  | Are all measures documented? | 2 | 6.1.3  |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Has the organisation’s chief executive ensured that roles and functions have been established with sufficient resources and expertise to perform the tasks necessary in order to fulfil the responsibility? | 2.1 | 5.3 |  |  | [ ] Yes [ ] No | PJL, Section 22GDPR, Article 24 first paragraphFLK, Section 7 | [ ] Yes [ ] No |
|  | Is it clear who is responsible, and what they are responsible for? | 2.1 | 5.3  |  |  | [ ] Yes [ ] No | GDPR, Article 24 first paragraphPJL, Section 22 and 23FLK, Section 7 | [ ] Yes [ ] No |
|  | Is everyone familiar with the tasks they are responsible for performing? | 2.1 | 5.3 |  |  | [ ] Yes [ ] No | PJL, Section 22 and 23GDPR, Article 24 first paragraph | [ ] Yes [ ] No |
|  | Does everyone possess sufficient knowledge of the relevant responsibilities and tasks of others? | 2.1 | 5.3 |  |  | [ ] Yes [ ] No | PJL, Section 22 and 23GDPR, Article 24 first paragraph | [ ] Yes [ ] No |
|  | Is everyone aware of who has authority to make decisions? | 2.1 | 5.3  |  |  | [ ] Yes [ ] No | GDPR, Article 24 first paragraphPJL, Section 23  | [ ] Yes [ ] No |
|  | Has the chief executive appointed a data protection officer if the organisation is a public sector organisation or a private sector organisation when the scope of data processing necessitates such an appointment? | 2.1 | 5.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 37(1) | [ ] Yes [ ] No |
|  | Will the data protection officer be given sufficient resources and access to appropriate expertise in order to perform his or her tasks? | 2.1 | 7.1\*7.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 38(2) | [ ] Yes [ ] No |
|  | Is the data protection officer free from all conflicts of interest with respect to any other roles that he or she performs within the organisation, and does the data protection officer not receive instructions regarding how his or her tasks are to be performed? | 2.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 38(3)(6) | [ ] Yes [ ] No |
|  | Has the organisation established a management system for information security and data protection (internal control)? | 2.4 | 4.4 |  |  | [ ] Yes [ ] No | PJL, Section 23GDPR, Article 24 first paragraph | [ ] Yes [ ] No |
|  | Is the management system adapted to the organisation’s size, risks, characteristics and activities, the nature, scope and purpose of the data processing and the context in which it is carried out? | 2.4 | 4.3  |  |  | [ ] Yes [ ] No | GDPR, Article 24 and 32 | [ ] Yes [ ] No |
|  | Has the senior management made the management system known within the organisation?  | 2.4 | 5.1 |  |  | [ ] Yes [ ] No | FLK, Sections 3 and 7(d) | [ ] Yes [ ] No |
|  | Does the organisation allocate sufficient funding and resources to enable necessary activities to be carried out? | 2.4 | 7.1 |  |  | [ ] Yes [ ] No | PJL, Section 23  | [ ] Yes [ ] No |
|  | Is the management system documented? | 2.4 | 7.5.1 |  |  | [ ] Yes [ ] No | PJL, Section 23GDPR, Article 24 first paragraphFLK, Section 3 and 5 | [ ] Yes [ ] No |
|  | Are documents in the management system kept up to date on an ongoing basis and archived from the date on which the document is superseded by a new current version? | 2.4 | 7.5.2  |  |  | [ ] Yes [ ] No | FLK, Section 5(3) | [ ] Yes [ ] No |
|  | Does the controller consider whether information that may have safety implications should be removed prior to disclosure?  | 2.4 | A.8.2.3\* |  |  |  | PJL, Section 22 and 23 second paragraph |  |
|  | Is the documentation of risks and measures relating to information security secured in a corresponding way to personal health data in the event that risk would be entailed were unauthorised parties to become aware of such data? | 2.4 | 7.5.3  |  |  | [ ] Yes [ ] No | PJL, Sections 22 and 23 second paragraph | [ ] Yes [ ] No |
|  | Is documentation of risks and measures up to date and available at all times? | 2.4 | 8.2 8.3 |  |  | [ ] Yes [ ] No | GDPR, Article 24(1)FLK, Section 5 | [ ] Yes [ ] No |
|  | If the organisation is a public sector organisation, have goals been described and a strategy established for information security? | 2.4 | 6.2  |  |  | [ ] Yes [ ] No | EFF, Section 15 (1) |  |
|  | Does the organisation’s senior management review the organisation’s activities relating to information security and data protection at least once a year? | 2.5 | 9.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 24(1)FLK, Section 8 | [ ] Yes [ ] No |
|  | Are action plans adopted in order to remedy the situation, with deadlines and the delegation of responsibility if the review indicates that the level of risk to which the organisation is exposed is unacceptable? | 2.5 | 9.3 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22FLK, Section 6 | [ ] Yes [ ] No |
|  | Is the management’s review documented? | 2.5 | 9.3 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22FLK, Section 5GDPR, Article 5 nr.2 | [ ] Yes [ ] No |
|  | Has the organisation established technical and organisational measures that are appropriate in order to manage risk in a satisfactory manner? | 3 | 6.1.3 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32(1)(b) | [ ] Yes [ ] No |
|  | Are the measures to ensure confidentiality, integrity, availability and robustness in the information systems balanced? | 3 | 6.1.2 |  |  | [ ] Yes [ ] No | GDPR, Article 32 | [ ] Yes [ ] No |
|  | When evaluating an acceptable level of risk, is consideration given to technological developments, implementation costs and the nature, scope and purposes of the information processing and the context in which it is carried out? | 3 | 6.1.2 |  |  | [ ] Yes [ ] No | GDPR, Article 32(1) | [ ] Yes [ ] No |
|  | Is it taken into account, for example, the type and amount of personal data, the size of the business, and the complexity of the procession in the work on risk management?  | 3 | 6.1.1 |  |  |  | GDPR, Article 32(1) |  |
|  | Are appropriate technical and organisational measures selected on the basis of the organisation’s size, nature and scope of the processing of personal health data, patient safety, risks, etc.? | 3.1 | 6.1.1\*8.1\*  |  |  | [ ] Yes [ ] No | GDPR, Section 32 | [ ] Yes [ ] No |
|  | Does the organization ensure that there is a proportionality between the risk, and the cost of the measure?  | 3.1  | 6.1.3  |  |  |  | GDPR, Section 32  |  |
|  | Has the organisation determined an acceptable level of risk based on the minimum requirements of the Code concerning information security and any internal information security goals? | 3.2 | 6.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32EFF, Section 15 | [ ] Yes [ ] No |
|  | Are the following minimum requirements regarding confidentiality determined?:The organisation shall ensure that the duty of confidentiality is fulfilled and that unauthorised persons do not gain access to data. * prevent unauthorised access to personal health data and other information of significance to information security
* restrict access for authorised personnel according to their professional needs
* maintain an overview (logs) of everyone who has gained access to personal health data and other information of significance to information security
 | 3.2 | (A.9.2\*,A.10.1\*,A.11.1\*,A.11.2\*,A.12.4\*&A.13.2.4\*) |  |  | [ ] Yes [ ] No | PJL, Sections 15, 19 and 22HPL, Section 21PJF, Section 14GDPR, Article 9(2)(i) | [ ] Yes [ ] No |
|  | Have the following minimum requirements regarding integrity been established?:The organisation shall ensure that personal health data and other information of significance to information security is complete, updated and accurate.* log who has performed registrations, alterations, corrections and erasures
* prevent accidental or unauthorised alteration or erasure
* ensure that accurate personal health data is recorded for the right person
* ensure that personal health data is registered in accordance with relevant code lists and terminology
* ensure that personal health data are complete and updated
* prevent copies of data from becoming a source of outdated information
 | 3.2 | A.12.4\*A.9.2\* A.9.4.1\*A.12.3\* |  |  | [ ] Yes [ ] No | PJL, Section 22PJF, Section 14GDPR, Article 5 (1)(f) and 32 (1)(b)  | [ ] Yes [ ] No |
|  | Have the following minimum requirements regarding availability and robustness been established?:The organisation shall ensure that personal health data and other information of significance to information security is available at the right time.* ensure that personal health data is available according to professional need
* ensure appropriate and stable operation of information systems
* ensure that appropriate technical and organisational measures are in place which enable prevention, detection, scalability, management and restoration
* ensure that information systems are available in accordance with the organisation’s availability requirements
 | 3.2 | (A.9.2\*,A.12.1\*,A.12.4.1\*,A.17.1\*&A.17.2\*) |  |  | [ ] Yes [ ] No | PJL, Section 19 first paragraphPJL, Section 22PJF, Section 14 third paragraphGDPR, Article 5 (1)(f) and 32 (1)(b) | [ ] Yes [ ] No |
|  | Are breaches of the requirements regarding confidentiality, integrity, accessibility and robustness processed as breaches? | 3.2 | A.16.1 |  |  | [ ] Yes [ ] No | GDPR, Article 33 | [ ] Yes [ ] No |
|  | Has the organisation prepared a record of the processing of personal health data? | 3.3 | A.8.1.1\* |  |  | [ ] Yes [ ] No | GDPR, Article 30 |  |
|  | Does the organisation have an overview of ICT systems, infrastructure, digital services and other information of significance to information security, etc.? The overview should be documented | 3.3 | A.8.1.1 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21FLK, Section 6 | [ ] Yes [ ] No |
|  | Does the organisation carry out risk assessments and assess the probability and potential consequences of an incident occurring?  | 3.4 | 6.1.2 |  |  | [ ] Yes [ ] No | GDPR, Section 32FLK, Section 6 | [ ] Yes [ ] No |
|  | If the risk is unacceptable, does the organisation implement measures to reduce the risk? | 3.4 | 6.1.38.3 |  |  | [ ] Yes [ ] No | GDPR, Section 32FLK, Section 7 | [ ] Yes [ ] No |
|  | Are risk assessments carried out at least before:* establishment of or changes to the processing of personal health data
* establishment of new systems or data filing systems which contain or use personal health data
* establishment of organisational, technical or other changes of significance tor information security
* access is established to health data between organisations
 | 3.4 | 6.1.2\*8.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 32(1)FLK, Section 6  | [ ] Yes [ ] No |
|  | Does the organisation’s management regularly carry out risk assessments as part of its efforts to monitor information security? | 3.4 | 8.2 |  |  | [ ] Yes [ ] No | GDPR, Article 24FLK, Section 8 | [ ] Yes [ ] No |
|  | Are risk assessments carried out on the basis of the minimum requirements regarding confidentiality, integrity, availability and robustness, and cross-checked against the organisation’s acceptable level of risk? | 3.4 | 8.2 |  |  | [ ] Yes [ ] No | GDPR, Articles 24 and 32FLK, Section 8 | [ ] Yes [ ] No |
|  | Is decisive consideration given in risk assessments to the consequences for patients/healthcare users and appropriate healthcare? | 3.4 | 6.1.2\* |  |  | [ ] Yes [ ] No | HRL, Section 21  |  |
|  | Are the risk assessments documented? | 3.4 | 8.2 |  |  | [ ] Yes [ ] No | PJL, Section 23GDPR, Article 5(2) and 24 (1) FLK, Section 5 | [ ] Yes [ ] No |
|  | When it is necessary to implement measures in order to achieve an acceptable level of risk, are the measures presented in a plan with clear deadlines and the names of the persons who are responsible for implementation? | 3.4 | 6.1.3 |  |  | [ ] Yes [ ] No | FLK, Section 5 and 6  | [ ] Yes [ ] No |
|  | Is the plan for the measures anchored in the organisation’s management? | 3.4 | 5.1 |  |  | [ ] Yes [ ] No | FLK, Section 3 | [ ] Yes [ ] No |
|  | Does the organisation have sufficient expertise at its disposal in order to carry out risk assessments? | 3.4 | 7.2 |  |  | [ ] Yes [ ] No | FLK, Section 7 | [ ] Yes [ ] No |
|  | Does representatives of healthcare personell sought involved where appropriate?  | 3.4 | 6.1.2\* |  |  |  | PJL, Section 22HRL, Section 21GDPR, Article 32 |  |
|  | Do persons who carry out risk assessments have a clear escalation path to the management/board? | 3.4 | 5.3  |  |  | [ ] Yes [ ] No | FLK, Section 8 | [ ] Yes [ ] No |
|  | Are the results of the risk assessment and a plan for the follow-up of measures communicated with the appropriate level of detail to the organisation's management and the board, as and when relevant? | 3.4 | 7.4\* |  |  | [ ] Yes [ ] No | FLK, Section 9  | [ ] Yes [ ] No |
|  | Do organisations always evaluate the consequences that the processing of personal health data will entail for data subjects? | 3.5 | 6.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 35(1) |  |
|  | Does the organisation document the lawfulness and purpose of the processing, the way in which the privacy of the data subject is safeguarded, and that sufficient measures have been implemented in order to manage the risks? | 3.5 |  |  |  | [ ] Yes [ ] No | GDPR, Section 35(1) |  |
|  | If it is likely that processing will entail a high level of risk for the data subjects concerned, does the organisation carry out a more thorough impact assessment as regards data protection, also known as a ‘DPIA’? | 3.5 |  |  |  | [ ] Yes [ ] No | GDPR, Section 35(1) | [ ] Yes [ ] No |
|  | Are data protection impact assessments carried out before the processing of personal data commences? | 3.5.1 |  |  |  | [ ] Yes [ ] No | GDPR, Section 35(1) |  |
|  | Is a data protection impact assessment carried out when a high risk as regards data protection will result?:* when health data is processed on a large scale
* if new technology is used
* when personal data is processed in an automated, systematic and comprehensive manner, as a basis for decisions which have legal effect or a significant impact on the data subject
* as a result of the nature, scope and purpose of the processing and the context in which it is carried out

[Consult the Norwegian Data Protection Authority for a list of when data protection impact assessments must be carried out](https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/) | 3.5.1 |  |  |  | [ ] Yes [ ] No | GDPR, Section 35(1) |  |
|  | Does the data protection impact assessment include at least the following:* a systematic description of the processing activities involving personal health data
* a description of the purpose of the processing of personal data
* an assessment of whether or not the processing of personal health data is necessary and proportionate to the purpose
* an assessment of the data protection risks for the data subject
* planned risk mitigation measures in order to safeguard data protection
 | 3.5.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 35(7) |  |
|  | Is the data protection officer, if one has been appointed, consulted when the data protection impact assessment is carried out? | 3.5.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 39(c) | [ ] Yes [ ] No |
|  | Are measures planned which reduce the risk regarding data protection in relation to the data protection impact assessment? | 3.5.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 35 | [ ] Yes [ ] No |
|  | If the processing of personal health data will entail a high level of risk which cannot be mitigated through reasonable means, does the controller consult the Norwegian Data Protection Authority before the processing commences? | 3.5.1 | A.6.1.3\*  |  |  | [ ] Yes [ ] No | GDPR, Article 36 | [ ] Yes [ ] No |
|  | Is the basis for processing established prior to commencement of the processing of personal health data, or in the event of changes to the processing? | 4.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 5 (1)(a) and 6  |  |
|  | Does the basis for processing cover all types of processing that is performed: collection, recording, storage, erasure, disclosure, etc.? | 4.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 6 |  |
|  | Is the basis for processing documented? | 4.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 5(2) |  |
|  | Has the organisation facilitated technical and organisational measures to ensure that data subjects are able to assert their rights? | 4.2 |  |  |  | [ ] Yes [ ] No | GDPR, Articles 12, 13, 15, 24 and 32 |  |
|  | Does the organisation ensure that all personnel who are granted access to personal health data and other information of significance to information security are familiar with their duty of confidentiality? | 4.2.1 | A.13.2.4 |  |  | [ ] Yes [ ] No | PJL, Section 15 and 16HPL, Section 21 and 21(a)GDPR, Article 9(2)(i)FLK, Section 7 | [ ] Yes [ ] No |
|  | Does the organisation ensure that personnel fulfil their duty of confidentiality? | 4.2.1 | 5.1\*A.7.2.1\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21 |  |
|  | Are breaches of the duty of confidentiality processed as a breaches? | 4.2.1 | A.7.2.3\*A.16.1\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22FLK, Section 9GDPR, Articles 33 and 34 | [ ] Yes [ ] No |
|  | Does the organisation provide information to data subjects in a concise, transparent, understandable and readily accessible manner, and in clear and simple language? | 4.2.2 |  |  |  | [ ] Yes [ ] No | GDPR, Article 12 |  |
|  | Is the information given to the data subject in writing or otherwise, including electronically if appropriate? | 4.2.2 |  | Patient rights |  | [ ] Yes [ ] No | GDPR, Article 15(3)EFF, Section 3 |  |
|  | Is the data subject only given the information verbally when the data subject identifies themselves? | 4.2.2 |  |  |  | [ ] Yes [ ] No | GDPR, Article 12 |  |
|  | When collecting information, does the controller inform the data subject, in an understandable manner, of their rights and how the personal data is processed? | 4.2.2 |  |  |  | [ ] Yes [ ] No | GDPR, Article 13 and 14 |  |
|  | Does the organisation ensure that the data subject is able to gain access to data that has been recorded about them? | 4.2.3 |  | Patient rights |  | [ ] Yes [ ] No | PJL, Section 18PJF, Section 11PBL. Section 5-1GDPR, Article 15 |  |
|  | Does access also result in a log of the names and organisations of persons who have obtained information, and what information they obtained and when? | 4.2.3 | A.12.4.1\* | Patient rights |  | [ ] Yes [ ] No | PJL, Section 18 first paragraphPBL, Section 5-1, first paragraph |  |
|  | Does the organisation ensure that data subjects are able to find out what personal data about themselves the organisation processes?This also includes finding out the names of persons from other organisations who have obtained the information | 4.2.3 | A.8.1.1\* |  |  | [ ] Yes [ ] No | PJL, Section 18PJF, Section 11GDPR, Article 15 |  |
|  | Does the organisation ensure that anyone who invokes their rights is identified? |  |  |  |  | [ ] Yes [ ] No | PJL, Section 13 |  |
|  | Does patients, that normally is entitled to gain access to all data in personal health data and personal data filing systems for therapeutic purposes about themselves?  | 4.2.3.1 |  |  |  | [ ] Yes [ ] No | PJL, Section 18HRL, Section 24PBL, Section 5-1 |  |
|  | Upon request, do healthcare professionals provide an explanation of specialist terms, etc.? | 4.2.3 |  |  |  | [ ] Yes [ ] No | PBL. Section 5-1 |  |
|  | Has provision been made to enable Sami-speaking, foreign language-speaking and disabled persons to exercise their right of access? | 4.2.3 |  |  |  | [ ] Yes [ ] No | PJF, Section 11 |  |
|  | Is it documented that provision been made to enable Sami-speaking, foreign language-speaking and disabled persons to exercise their right of access? | 4.2.3 |  |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22 |  |
|  | Are patients denied access to all or certain information in a medical record if it is absolutely necessary in order to prevent risk to life or severe injury for the patient themselves, or if access is obviously inadvisable out of consideration for persons who are close to the person concerned? | 4.2.3 |  |  |  | [ ] Yes [ ] No | PBL. Section 5-1 |  |
|  | Does the controller give access within 30 days at no cost to the patient? | 4.2.3 |  |  |  | [ ] Yes [ ] No | GDPR, Article 12 (3) and 5 |  |
|  | Does correction take place through re-entry or through the addition of a dated correction in the medical record?(Corrections shall not be made through the erasing of information) | 4.2.4.1 | A.9.1.1\* | Patient rights |  | [ ] Yes [ ] No | HPL, Section 42 |  |
|  | As a general rule, is correction and erasure carried out by the person who signed the information? | 4.2.4.1 | A.9.1.1\* |  |  | [ ] Yes [ ] No | PJF, Section 15 |  |
|  | Is correction or erasure performed by a healthcare professional appointed by the controller, when the person who signed it is unable to do it? | 4.2.4.1 | A.9.1.1\* |  |  | [ ] Yes [ ] No | PJF, Section 15 |  |
|  | Is information that has been recorded under the wrong person erased unless there are compelling reasons in the public interest why erasure should not be carried out? | 4.2.4.1 | A.9.1.1\* | Patient rights |  | [ ] Yes [ ] No | HPL, Section 44 |  |
|  | Does the controller notify anyone who has received personal data which is subsequently corrected or erased?(Notification shall be given of any correction or erasure of personal data) | 4.2.4.1 |  |  |  | [ ] Yes [ ] No | GDPR, Article 17 |  |
|  | Does the controller notify the data subject of the abovementioned recipients if the data subject so requests? | 4.2.4.1 |  |  |  | [ ] Yes [ ] No | GDPR, Articles 13 and 14 |  |
|  | If a request for correction or erasure is denied, is the patient notified of their right of appeal? | 4.2.4.1 |  |  |  | [ ] Yes [ ] No | PJF, Section 15 |  |
|  | Does the organisation ensure that no data is transferred or made available if the patient or healthcare user objects?(Data may also not be transferred or released if there is reason to believe that the patient or healthcare user would object were they to be asked. Transfer and release may still take place if there are compelling reasons for such transfer or release) | 4.2.5.1 |  |  |  | [ ] Yes [ ] No | HPL, Section 25(1) first paragraph |  |
|  | Does the organisation ensure that the patient is made aware of this right to opt out? | 4.2.5.1 |  |  |  | [ ] Yes [ ] No | HPL, Section 10PBL, Sections 3-2, 3-3 and 3-4 |  |
|  | Is the name of the persons who receive information, and the organisation they belong to documented?  | 4.2.5.1 |  |  |  | [ ] Yes [ ] No | PJL, Section 25 |  |
|  | Does health personnel shall grant collaborating personnel access to necessary and relevant health data insofar as such access is necessary in order to provide a patient with healthcare in an appropriate manner, unless the patient or healthcare user objects? | 4.2.5.2 |  |  |  | [ ] Yes [ ] No | HPL, Section 25 |  |
|  | Is health data that is disclosed to the management not directly personally identifiable insofar as is possible? | 4.2.5.2 | A.8.2\* | Patient rights |  | [ ] Yes [ ] No | HPL, Section 26 first paragraph | [ ] Yes [ ] No |
|  | Is health data that is disclosed to the management limited to what is necessary and relevant for the intended purpose?  | 4.2.5.3 |  |  |  | [ ] Yes [ ] No |  |  |
|  | Do healthcare professionals enter the patient’s national ID number and data concerning diagnosis, any medical needs, services, admission and discharge dates and relevant administrative data in the organisation’s internal patient administration systems? | 4.2.5.4 |  |  |  | [ ] Yes [ ] No | HPL, Section 26 |  |
|  | Is health data that is made available for learning and quality assurance purposes limited to the data that is necessary and relevant to the healthcare professional's own learning or for the quality-assurance of healthcare? | 4.2.5.5 | A.8.2\*A.9.1\*A.9.2\* | Patient rights |  | [ ] Yes [ ] No | HPL, Section 29(c) |  |
|  | Does the patient’s record state what data has been disclosed and to whom it has been disclosed to? | 4.2.5.4 |  |  |  | [ ] Yes [ ] No | HPL, Section 29(c) |  |
|  | Is health data stored until there is no longer considered to be any need for it given the nature of the healthcare concerned? | 4.2.6.1 | A.8.1\* | Patient rights |  | [ ] Yes [ ] No | PJL, Section 25 | [ ] Yes [ ] No |
|  | Is data concerning who has gained access to or received health data which is linked to the name or national ID number of the patient or healthcare user concerned (logs) stored until there is no longer considered to be any need for it given the nature of the healthcare concerned? | 4.2.6.1 | A.8.1\* | Logging |  | [ ] Yes [ ] No | PJL, Section 25 | [ ] Yes [ ] No |
|  | Will the data then be erased if it is not to be retained under the Archive Act, the Health Archive Act or any other applicable legislation? | 4.2.6.1 | A.8.1.2\* | Patient rights |  | [ ] Yes [ ] No | PJL, Section 25 |  |
|  | Does the electronic personal health data filing system for therapeutic purposes always reflect the original after digitalisation? | 4.2.6.2 | A.8.1.3\* |  |  | [ ] Yes [ ] No | PJL, Section 16 |  |
|  | Do the organisation and suppliers consider data protection in every development phase of a system or solution? | 4.3 | A.14.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32 |  |
|  | Does the organisation ensure that the information systems follow the principles of data protection and safeguard the rights of data subjects? | 4.3 | A.14.1\*A.14.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 25 |  |
|  | Does the controller select suppliers which are able to provide services that fulfil statutory requirements and the requirements of the Code? | 4.3 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28(1) |  |
|  | Do suppliers assist any controller which uses their products and services in fulfilling these requirements?If necessary, do the parties have to enter into a dialogue to determine the appropriate measures in order to fulfil the requirements? | 4.3 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28  |  |
|  | Are all security measures suitable and chosen on the basis of risk assessments? | 5 | 6.1.3 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Does the organisation assess whether it is necessary to implement more comprehensive measures than those described in the Code? | 5 | 6.1.3 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 8 | [ ] Yes [ ] No |
|  | Do all employees in the organisation undergo continuous training regarding the requirement to fulfil the duty of confidentiality, information security and data protection? | 5.1.1 | 7.2\*7.3\*A.7.2.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7 | [ ] Yes [ ] No |
|  | Does the organisation obtain a confidentiality agreement for each employee? | 5.1.1 | A.7.1.2A.13.2.4 |  |  | [ ] Yes [ ] No | PJL, Section 15 and 23HRL, Section 22 | [ ] Yes [ ] No |
|  | Has the organisation guidelines for the private use of information systems and equipment?  | 5.1.1 | A.8.1.3 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22FLK, Section 7 | [ ] Yes [ ] No |
|  | Has the organisation established measures which ensure that everyone who is given access to information systems and related information possesses sufficient competence to use the systems and to safeguard information security and data protection regarding data subjects? | 5.1.2 | A.7.2.1A.7.2.2 |  |  | [ ] Yes [ ] No | PJL, Sections 22 and 23HRL, Sections 21 and 22FLK, Section 7 | [ ] Yes [ ] No |
|  | Is the training continuous and adapted to the various roles and user groups concerned? | 5.1.2 | A.7.2.2 |  |  | [ ] Yes [ ] No | PJL, Sections 22 and 23HRL, Sections 21 and 22FLK, Section 7 | [ ] Yes [ ] No |
|  | Are new training initiatives considered in the event of technological changes or change in procedures? | 5.1.2 | (A.7.2.2\*&A.12.1.2\*) |  |  | [ ] Yes [ ] No | PJL, Sections 22 and 23HRL, Sections 21 and 22FLK, Section 7 | [ ] Yes [ ] No |
|  | In the event of termination of employment, is all media (including digital, paper, etc.) which may contain health and/or personal data returned? | 5.1.3 | A.8.1.4 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Are access cards returned and deactivated in the event of termination of employment? | 5.1.3 | (A.8.1.4\*,A.9.2.6\*&A.11.1.2\*) |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is all access blocked in the event of termination of employment? | 5.1.3 | A.9.2.6 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Does the organisation have procedures in place for tidying up information which the employee may have stored in their own user account. | 5.1.3 | A.8.1.4\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22FLK, Section 7 | [ ] Yes [ ] No |
|  | Does the organisation have procedures for the authorisation, alteration and termination of access? | 5.2 | A.9.2.1A.9.2.2 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21PJF, Section 13 | [ ] Yes [ ] No |
|  | Within the framework of the duty of confidentiality, does the organisation ensure that relevant and necessary health data is available to health personnel and collaborating personnel as and when necessary in order to provide, administer or quality-assure the provision of healthcare to individuals? | 5.2 | A.9.2\* |  |  | [ ] Yes [ ] No | PJL, Sections 15 and19HPL, Sections 21 and 25GDPR, Article 32(1)(b) | [ ] Yes [ ] No |
|  | Does the organisation ensure that the data is made available in a manner which addresses information security and data protection? | 5.2 | A. 9. 1. 1\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Has access control been established for all information systems? | 5.2 | A. 9. 1. | Authorisation |  | [ ] Yes [ ] No | PJL, Section 22PJF, Section 13HFL, Section 7 first paragraphHPL, Section 25 second paragraphGDPR, 32(1)(b)  | [ ] Yes [ ] No |
|  | Has access control been established for administrator and system users? | 5.2 | A.9.2.3  | Authorisation |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Has it been ensured that only authorised personnel with a professional need may gain access to personal health data and personal data? | 5.2 | A.9.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is access to personal health data filing systems for therapeutic purposes (including electronic patient records/data processing systems) granted following a specific decision based on the completed or planned implementation of measures for the medical treatment of the patient?  | 5.2 | A.8.1.3\* | Authorisation |  | [ ] Yes [ ] No | PJL, Section 19 |  |
|  | Is access controlled to ensure compliance with the confidentiality rules and so that no access to personal health data is given to anyone other than those with a professional need to gain such access? | 5.2 | A.9.2\*A.9.4\* |  |  | [ ] Yes [ ] No | PJL, Sections 19 and 22HPL, Section 25PJF, Section 13 first paragraph (a) | [ ] Yes [ ] No |
|  | Is the statutory duty of confidentiality assessed and safeguarded in connection with the allocation of authorisation? | 5.2.1 | A.9.2.1\*A.9.4.1\* |  |  | [ ] Yes [ ] No | PJL, Sections 15 and 23PJF, Section 13 first paragraph (a), Section 15 | [ ] Yes [ ] No |
|  | Does allocated authorisation ensure that an individual employee is able to gain access to relevant personal health data as and when necessary in accordance with the employee’s responsibilities and duties, insofar as the statutory duty of confidentiality does not prevent such access? | 5.2.1 | A.9.2\* | Authorisation |  | [ ] Yes [ ] No | PJL, Sections 19 and 22PJL, Section 13 first paragraph | [ ] Yes [ ] No |
|  | Is the authorisation reviewed in the event of any changes in responsibilities, employment or long-term absence? | 5.2.1 | A.9.2.2 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | If roles are used within an organisation, does authorisation have to be granted for each role, irrespective of the employee’s other roles? | 5.2.1 | A.9.1\*A.9.2\* | Authorisation |  | [ ] Yes [ ] No | PJL, Section 13 | [ ] Yes [ ] No |
|  | Is authorisation for access to personal health data filing systems for therapeutic purposes time-limited? | 5.2.1 | A.9.2.2\* | Authorisation |  | [ ] Yes [ ] No | PJF, Section 13 | [ ] Yes [ ] No |
|  | Does authorisation for access to personal health data filing systems for therapeutic purposes specify which organisations the authorisation covers? | 5.2.1 | A.9.1\*A.9.2\* | Authorisation |  | [ ] Yes [ ] No | PJF, Section 13 | [ ] Yes [ ] No |
|  | Have measures been established so that any misuse by authorised technical personnel with a specific need to access large quantities of personal health data will be detected? | 5.2.1 | A.12.4.3 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21FLK, Section 7 | [ ] Yes [ ] No |
|  | Is the reason for self-authorisation recorded? | 5.2.1 | A.12.4\*A.16.1\*  | Authorisation |  | [ ] Yes [ ] No | PJL, Section 19 second paragraph | [ ] Yes [ ] No |
|  | Have technical measures been established to ensure that persons inside or outside the organisation are unable to alter data without the name of the person who made the change and what has been changed being logged in the information systems?Examples of the requirement where PKI is not used: Password files shall be encrypted | 5.2.1 | A.12.4.1 | Authentication |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is all allocation of authorisation recorded in an authorisation log? | 5.2.1 | A.9.2.1\* | Authorisation |  | [ ] Yes [ ] No | PJF, Section 13 first paragraph (c) | [ ] Yes [ ] No |
|  | Have technical measures been established to ensure that persons outside the organisation are unable to alter configurations and software without the changes being logged? | 5.2.1 | A.12.4.3 | Logging |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Does a user with administration rights use personal separate user accounts for administration tasks? | 5.2.1 | A.9.2.3 | Authorisation |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Do operating personnel have personal users for tasks which do not require administrator rights? | 5.2.1 | A.9.2.3 | Authorisation |  |  | GDPR, Section 32PJL, Section 22HRL, Section 21 |  |
|  | Have different administrator users been established for the various parts of the infrastructure that are managed? | 5.2.1 | A.9.2.3 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Has a risk assessment been carried out which justifies the need for different administrator users? | 5.2.1 | (A.2\* & A.9.2.3\*) |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Has the organisation ensured that an authorisation log is created which at least contains the following:* information on who has been allocated authorisation
* the role to which the authorisation has been allocated (if roles are used by the organisation)
* purpose of the authorisation
* time at which the authorisation was given and revoked (where applicable)
* information on the organisation to which the authorised person is linked
* authorisation of health personnel regarding access to health data in other organisations (only if access to health data in other organisations is in use)

Examples of the requirement: It shall also be logged who (a physically identifiable person) created (logged) the authorisation | 5.2.1.1 | A.9.2.1\* | Authorisation |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21PJF, Section 13 first paragraph (c) | [ ] Yes [ ] No |
|  | Does the organisation have control and oversight over the processing of personal health data and personal data for which they are responsible?  | 5.2.1.2 | A.8.1.1\* |  |  | [ ] Yes [ ] No | GDPR, Articles 30 and 5 (2)  | [ ] Yes [ ] No |
|  | Does the organisation have an overview of the release of data to other organisations? | 5.2.1.2 | A.8.1.1\*A.13.2.2\* | Logging |  | [ ] Yes [ ] No | PJL, Section 13 first paragraph (b) | [ ] Yes [ ] No |
|  | Is a risk assessment carried out in the event of the new provision or changes to the existing disclosure of information to other organisations? | 5.2.1.2 | 8.2\* |  |  | [ ] Yes [ ] No | PJL, Section 19 second paragraph | [ ] Yes [ ] No |
|  | Have controllers and organisations that are given access to data held by the controller clarified, through an agreement or otherwise, how:* authentication is to take place securely
* authorisation for health data held by the controller is to be granted
* logging and follow-up of logs is to take place
 | 5.2.1.2 | A.13.2.2\*A.9.1\*A.9.2\*A.12.4\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21 |  |
|  | Do authorised persons verify their identity in a secure manner? | 5.2.2 | A.9.4.2 | Authentication |  | [ ] Yes [ ] No | PJF, Section 13 second paragraph | [ ] Yes [ ] No |
|  | Is the secure manner determined on the basis of a risk assessment? | 5.2.2 | 8.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Are different employment relationships identified through authentication?  | 5.2.2 | A.9.1 | Authentication |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is it ensured that several people cannot use the same authentication criteria?Clarification of the requirement where PKI is not used: * It shall be easy for the user to change the password
* Enforced password changes shall be technically possible
* It shall be possible to configure the quality and duration of the password
 | 5.2.2 | A.9.4 | Authentication |  | [ ] Yes [ ] No | PJF, Section 13 second paragraph | [ ] Yes [ ] No |
|  | Are authentication criteria (such as user name and password) allocated in an appropriate manner? | 5.2.2 | (A.9.2.2\*,A.9.2.3\*&A.9.2.4\*) |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21PJF, Section 13 second paragraph | [ ] Yes [ ] No |
|  | Is access from home offices and/or mobile equipment (and mobile networks) secured through a secure authentication solution? | 5.2.2 | (A.6.2.2\*&A.9.4.2\*) |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21PJF, Section 13 second paragraph | [ ] Yes [ ] No |
|  | Are all default passwords (factory settings) on systems and equipment changed before the processing of personal health data is commenced? | 5.2.2 | A.9.4.3\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | When using wireless networks for processing personal health data, is the authorised user authenticated using a secure authentication solution? | 5.2.2 | (A.9.1.2\*&A.9.4.2\*) | Authentication |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21PJF, Section 13 second paragraph | [ ] Yes [ ] No |
|  | Is the individual role identified if roles are used?  | 5.2.2 | A.9.1.1\* | Authentication |  | [ ] Yes [ ] No |  | [ ] Yes [ ] No |
|  | Is re-authentication approved if necessary when changing role (if roles are used)? | 5.2.2 | A.9.4.2\* | Authentication |  | [ ] Yes [ ] No |  | [ ] Yes [ ] No |
|  | Does the organisation’s management ensure that regular checks are carried out to determine who has gained electronic access?Examples of the requirement: Personal health data filing system for therapeutic purposes must have functionality to ensure that the control can be carried out effectively. | 5.2.3 | A.9.2.5 | Authorisation |  | [ ] Yes [ ] No | GDPR, Sections 32 and 5 (1)(f)PJL, Section 22HRL, Section 21PJF, Section 13 first paragraph (e) and third paragraph | [ ] Yes [ ] No |
|  | Do individual managers conduct reviews and checks on access management, including allocated authorisations?:* in the event of organisational changes, transfer of personnel to another unit/department or change in duties?
* At least once a year (ideally in connection with security audits)?
* In the event of a security breach within the information area that is affected by the breach?
 | 5.2.3 | (A.9.2\*,A.12.1.2\*&A.17.1.3\*) |  |  | [ ] Yes [ ] No | PJL, Sections 22 and 23HRL, Sections 21 and 22PJF, Section 13 first paragraph (e) and third paragraph | [ ] Yes [ ] No |
|  | Is the organisation’s management informed if checks lead to a suspicion that unauthorised access has taken place? | 5.2.3 | A.16.1.5 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22 | [ ] Yes [ ] No |
|  | If the checks reveal that unauthorised access has taken place, is this processed as a breaches? | 5.2.3 | A.16.1.4 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 33 | [ ] Yes [ ] No |
|  | Is the misuse of self-authorisation followed up as a breaches? | 5.2.3 | A.12.4\*A.16.1\*A.7.2.3\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22 | [ ] Yes [ ] No |
|  | In the event of access being gained to health data across organisations, do the contractual parties collaborate regarding access management? | 5.2.3 | A.13.2.2\*A.15.1\*A.15.2\*A.9.2.5\* |  |  | [ ] Yes [ ] No | PJL, Section 9 first paragraph (c) | [ ] Yes [ ] No |
|  | Does a controller who has access to authorise health personnel for access between organisations continually monitor:* who within his or her own organisation has electronically retrieved health data from another organisation
* why this was done
* the period of time during which the health data was retrieved
 | 5.2.3 | A.13.2.2\*A.15.2\*A.12.4.1\*A.16.1\* | Authorisation |  | [ ] Yes [ ] No | PJL, Section 14 | [ ] Yes [ ] No |
|  | Is the organisation from which the data was obtained and the patient/healthcare user that the data concerns notified if the checks indicate that an unauthorised person has retrieved health data? | 5.2.3 | A.13.2.2\*A.16.1\* |  |  | [ ] Yes [ ] No | PJF, Section 14 third paragraph | [ ] Yes [ ] No |
|  | Is the patient/healthcare user notified by the organisation from which the data was obtained if the checks indicate that an unauthorised person has retrieved health data? | 5.2.3 | A.16.1\* |  |  | [ ] Yes [ ] No | GDPR, Article 34 |  |
|  | Is the breaches (concerning the unauthorised retrieval of health data) processed in accordance with established procedures for breaches management? | 5.2.3 | A.16.1\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 33 | [ ] Yes [ ] No |
|  | Has a procedure been established for the administration of keys/access cards in the access management system? | 5.3.1 | A.11.1.2 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Section 32 | [ ] Yes [ ] No |
|  | Have security measures been established which prevent unauthorised access to personal health data?This can be solved through access management to premises using equipment and through protecting the ICT equipment against misuse or unauthorised access. | 5.3.2 | A.11.1 |  |  | [ ] Yes [ ] No | PJL, Sections 22 and 23HRL, Sections 21 and 22GDPR, Sections 32 and 5(1)(f) | [ ] Yes [ ] No |
|  | Have security measures been established which ensure that only authorised personnel are able to gain access to such infrastructure? | 5.3.3 | A.11.1 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32 | [ ] Yes [ ] No |
|  | Are all storage media erased appropriately as and when they are taken out of use? | 5.3.3 | (A.8.3.2\*&A.11.2.7\*) |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Articles 17 and 32 | [ ] Yes [ ] No |
|  | Are risk assessments carried out concerning the solutions that are used for mobile equipment and home offices before the solutions are taken into use and in the event of changes that could impact on information security? | 5.3.4 | A.11.2.6\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Have administrative procedures been established regarding the use of mobile equipment and home offices? | 5.3.4 | A.6.2 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 23HRL, Section 22 | [ ] Yes [ ] No |
|  | Is personal health data only stored locally as and when necessary based on professional need and encrypted? | 5.3.4 | A.8.1.3\*A.8.2.3\*A.10.1.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Have technical measures been established so that all communication of personal health data outside the control of the organisation is encrypted? | 5.3.5 | A.10.1\*A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is encryption and decryption between communication points in the infrastructure performed by approved equipment over which the organisation has control?This control may be addressed through an agreement. | 5.3.5 | A.10.1\*A.13.1.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is all communication, whether wireless or wired, encrypted? | 5.3.5 | (A.10.1\*&A.13.2\*) |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is stored directly identifiable personal data which is processed in accordance with Sections 10 and 11 of the Personal Health Data Filing System Act encrypted? | 5.3.5 | A.8.1.3\*A.8.2.3\*A.10.1.1\* |  |  | [ ] Yes [ ] No | HRL, Section 21GDPR, Section 32 | [ ] Yes [ ] No |
|  | Is medical equipment which processes personal health data covered by the organisation’s efforts relating to information security and data protection, e.g. in risk assessments, access control, change control and procedures regarding use, in the same way as other information systems? | 5.3.6 | (A.11.2\*,A.14.1.1\*,A.9.4\*,A.14.2.2\*&A.8.1.3\*) |  |  | [ ] Yes [ ] No | PJL, Section 22GDPR, Section 32Section 11 of Forskrift om håndtering av medisinsk utstyr (the Medical Devices Regulation) | [ ] Yes [ ] No |
|  | Does the configuration ensure that the equipment and software only perform the functions that are specific to the intended purpose? | 5.4.1 | (A.12.5.1\*&A.14.2.2\*) |  |  | [ ] Yes [ ] No | GDPR, Section 32 and 25PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Does the organisation ensure that all data flow, data communication and integrations are mapped and documented? | 5.4.1 | A.12.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Sections 7 and 5 | [ ] Yes [ ] No |
|  | Is it ensured that only approved equipment and software is used for the processing of personal health data? | 5.4.1 | A.12.6.2\*A.8.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21EFF, Section 17 | [ ] Yes [ ] No |
|  | Has the organisation stipulated who approves equipment and software that is used to process personal health data? | 5.4.1 | A.12.5.1\*A.6.1.1\*A.8.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7 | [ ] Yes [ ] No |
|  | Are hardware and software updated so that the latest and most modern security functionality is provided and necessary security measures are implemented? | 5.4.1 | A.12.6 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 15 | [ ] Yes [ ] No |
|  | Do scheduled changes follow the organisation’s procedure for configuration changes? | 5.4.1 | A.14.2.2 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 17EFF, Section 15 | [ ] Yes [ ] No |
|  | Are separate environments used for development, testing and production, so that personal health data used in the provision of healthcare is not affected by any errors which occur during development and testing? | 5.4.1 | A.12.1.4 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Is the configuration of equipment and software checked regularly to ensure that it only performs the intended functions? | 5.4.1 | (A.12.1.1\*&A.12.5.1\*) |  |  | [ ] Yes [ ] No | GDPR, Section 32 and 25PJL, Section 22HRL, Section 21FLK, Section 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Is the configuration protected from malware? | 5.4.1 | A.12.2.1 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is the configuration protected from unintended events? | 5.4.1 | A.14.2.2\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32 | [ ] Yes [ ] No |
|  | Are configuration changes, i.e. changes to equipment and/or software, only taken into use when:* A risk assessment has been carried out which demonstrates that an acceptable level of risk is achieved?
* A test has been carried out which ensures that the expected functions are performed?
* Implementation has been carried out which provides protection against unforeseen events?
* New configuration has been documented?
* Configuration changes have been approved by the organisation’s manager or the person designated by the management?
 | 5.4.2 | A.14.2 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 5 and 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Are configuration checks regulated through an agreement concerning:* Use by a processor?
* Use of remote access for maintenance and updates (Remote access shall only be gained via channels over which the organisation has control)?
 | 5.4.2 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 28 and 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Are all changes of significance to information security within the organisation, information systems and infrastructure anchored at the relevant managerial level? | 5.4.3 | (A.12.1.2\* &5.1\*) |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22FLK, Sections 3 and 7 | [ ] Yes [ ] No |
|  | Has the organisation established procedures for change management, which encompass the following topics:* Identification of material changes
* Planning and testing of changes
* assessment of potential consequences, for example by conducting a risk assessment and, where appropriate, a data protection impact assessment
* Approval procedure for changes?
* Communication of plan to relevant persons/roles
* Back-up procedures if the change has to be cancelled or fails or incidents occur
* Change log with relevant information
* Training of relevant users/roles
 | 5.4.2 | A 12.1.2 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Articles 32 and 35FLK, Sections 6 and 7 | [ ] Yes [ ] No |
|  | Does the organisation’s management ensure that back-ups are made of personal health data as well as other information that is necessary for the restoration of normal operation? | 5.4.4 | A.12.3.1 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Are back-ups stored in a locked and fire-proof facility and kept separate from operating equipment? | 5.4.4 | A.12.3.1 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7 | [ ] Yes [ ] No |
|  | Are regular tests carried out to ensure that back-ups are correct and can be restored? | 5.4.4 | A.12.3.1 |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Sections 7 and 8 | [ ] Yes [ ] No |
|  | Is at least one back-up protected against malware and incidents? | 5.4.4 | A.12.3.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Is at least the following logged:* Authorised use of information systems
* All system and administrator use for information systems and infrastructure
* Configuration and software changes
* Security-relevant incidents in security barriers
* Attempted unauthorised use of information systems and infrastructure
* Use of self-authorisation
 | 5.4.4 | A.12.4\* | Logging |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32PJF, Section 14 | [ ] Yes [ ] No |
|  | Is at least the following recorded in the logs in the event of the authorised use of personal health data filing systems for therapeutic purposes:* Identity of the person who retrieved health data
* Organisational affiliation of the person who retrieved the health data
* The basis for the disclosure
* The time period for the disclosure
 | 5.4.4 | A.12.4.1\* | Logging |  | [ ] Yes [ ] No | PJF, Section 14 first paragraphHPL, Section 45 first paragraph | [ ] Yes [ ] No |
|  | Are the requirements in the case of the processing of personal health data for purposes other than the provision of healthcare and care services determined on the basis of a risk assessment? | 5.4.4 | 8.2\*A.12.4.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7 | [ ] Yes [ ] No |
|  | Can logs readily be analysed using analysis tools with the aim of detecting breaches? | 5.4.4 | A.12.4.1\* |  |  | [ ] Yes [ ] No | PJF, Section 14 third paragraph | [ ] Yes [ ] No |
|  | Have procedures been established to analyse the logs to ensure that incidents are detected before they have serious consequences? | 5.4.4 | A.12.4.1\*A.12.4.3\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 23HRL, Section 22 | [ ] Yes [ ] No |
|  | Is it handled as a breach, if the breach is detected by analysing the logs?  | 5.4.4 | A.16.1\* |  |  | [ ] Yes [ ] No | PJL, Section 22 and 14HRL, Section 21GDPR, Articles 33 and 34 | [ ] Yes [ ] No |
|  | Have procedures been established to ensure that logs can be compared with the authorisation log as and when necessary? | 5.4.4 | A.12.4.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 23HRL, Section 22PJF, Section 13 | [ ] Yes [ ] No |
|  | Are logs protected against alteration and erasure by unauthorised personnel? | 5.4.4 | A.12.4.2A.12.4.3 | Logging |  | [ ] Yes [ ] No | GDPR, Articles 5 (1)(f) and 32PJL, Section 22HRL, Section 21PJF, Section 13 and 15 | [ ] Yes [ ] No |
|  | Do logs have a correct timestamp? | 5.4.4 | A.12.4.1A.12.4.4 | Logging |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21PJF, Section 14 | [ ] Yes [ ] No |
|  | Are logs generated in connection with the provision of healthcare stored until it is considered that there is no longer any use for them? | 5.4.4 | 12.4.2\* | Logging |  | [ ] Yes [ ] No | PJL, Section 25 | [ ] Yes [ ] No |
|  | Do management and handling of technical vulnerabilities follow the relevant procedures for change management? | 5.4.5 | (A.12.6.1\* & A.12.1.2\*) |  |  | [ ] Yes [ ] No | PJL, Section 23 first paragraphFLK, Section 7 | [ ] Yes [ ] No |
|  | Does the organisation have procedures for obtaining information concerning technical vulnerabilities in equipment and software? | 5.4.5 | A.12.6.1 |  |  | [ ] Yes [ ] No | PJL, Section 23 first paragraphFLK, Section 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Have procedures and operational measures been established which address:* Responsibility for: monitoring, risk assessment, correction and coordination
* How the organisation should respond to and report vulnerabilities
* Prioritisation and establishment of time line for correction
 | 5.4.5 | (A.12.6.1\*,A.12.1.2\*&A.16.1.5\*) |  |  | [ ] Yes [ ] No | PJL, Section 23 first paragraphGDPR, Article 32FLK, Section 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Does the organisation’s management follow up to ensure that security is being safeguarded through regular and at least annual security audits? | 5.4.6 | 9.2\* |  |  | [ ] Yes [ ] No | PJL, Section 23 first paragraphGDPR, Article 32(1)(d)FLK, Section 8 | [ ] Yes [ ] No |
|  | Is there an approved plan for security audits? | 5.4.6 | 9.2 |  |  | [ ] Yes [ ] No | PJL, Section 23 first paragraphGDPR, Article 32(1)(d)FLK, Section 6 | [ ] Yes [ ] No |
|  | Are results, conclusions and breaches derived from security audits documented and dealt with by the organisation? | 5.4.6 | (9.2\* & 10.1\*) |  |  | [ ] Yes [ ] No | PJL, Section 23, second paragraphFLK, Section 5 and 8 | [ ] Yes [ ] No |
|  | Has the organisation clearly defined the requirements that apply to network security, and the measures that have been implemented based on a risk assessment? | 5.5.1 | (A.13.1\* & 6.1.2\*) |  |  | [ ] Yes [ ] No | PJL, Section 22, first paragraphHRL, Section 21GDPR, Article 32(1)(b) and 35FLK, Section 6 and 7 | [ ] Yes [ ] No |
|  | In the case of connections to networks which are located outside the organisation, have technical measures been established which ensure that:* Only explicitly permitted traffic may pass from the outside in or vice versa; all other traffic is stopped
* The measures shall include at least two independent technical measures to ensure that persons outside the organisation are unable to gain unauthorised access to and/or alter or erase personal health data
 | 5.5.2 | A.13.1\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32(1)(b)FLK, Section 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Has clear responsibility been established between the sender, recipient and any message mediator in the event of message mediation? | 5.5.3.1 | A.13.2 |  |  | [ ] Yes [ ] No | FLK, Sections 3, 7 and 8 | [ ] Yes [ ] No |
|  | Have all agreements regarding message mediation been established in writing? | 5.5.3.1 | A.13.2.2 |  |  | [ ] Yes [ ] No |  | [ ] Yes [ ] No |
|  | Has it been agreed that the tendering organisation shall be responsible for:* its own connection security which prevents unauthorised access and penetration
* ensuring that the service cannot disseminate software which contain malware or similar
* secure transmission encryption end-to-end
 | 5.5.3.1 | A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Has it been agreed that the user organisation shall be responsible for:* ensuring that the service cannot disseminate software which contain malware or similar
* its own connection security which prevents unauthorised access and penetration
* ensuring secure transmission encryption end-to-end
 | 5.5.3.1 | A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | ensuring that, as and when necessary, the message is signed in such a way that the organisation cannot deny that it sent it* correct addressing of electronic interaction messages in accordance with the address register
* ensuring that, as and when necessary, the message is signed in such a way that the organisation cannot deny having sent it
* breaches reporting in connection with erroneous sending
* ensuring that messages are delivered in the agreed format
 | 5.5.3.2 | A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21EFF, Section 27 | [ ] Yes [ ] No |
|  | In connection with message communication based on the ebXML framework, has it been agreed that the recipient shall be responsible for:* logging receipt as and when necessary, so that the recipient cannot deny having received the message
* breaches reporting in connection with errors, i.e. receipt of a message which is not addressed to the organisation
* ensuring that messages are received in the agreed format
 | 5.5.3.2 | A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21EFF, 27 | [ ] Yes [ ] No |
|  | In connection with message communication based on the ebXML framework, has it been agreed that the message mediator shall be responsible for:* ensuring that messages are only delivered to the addressee
* ensuring that messages cannot be altered or destroyed during transport from the sender to the recipient
* ensuring that messages cannot be read by anyone other than the sender and recipient
* ensuring that messages are delivered by the agreed deadlines following dispatch
* breaches reporting in connection with all the above points
 | 5.5.3.2 | A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7 | [ ] Yes [ ] No |
|  | Are the following security principles followed in connection with data sharing:* There must be secure user authentication (consumer authentication) which is trusted by organisations that offer data sharing interfaces
* Any organisation that requests access shall verify that the user (consumer) has the necessary authorisations for the data sharing interface concerned
* A distinction shall be made between read and write rights for different information elements based on the individual user authorisation
* Unnecessary intermediate storage shall be avoided
* It shall be possible for clients to verify the legitimacy of the data sharing interface and the organisation that is offering it
* Common components for consumer authentication shall be used where available and expedient
 | 5.5.3.3 | A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 7EFF, Section 15 | [ ] Yes [ ] No |
|  | Has the organisation established measures to prevent personal health data and other information of importance to information security from being disclosed through the use of unencrypted e-mail and SMS or other insecure channels? | 5.5.4 | A.13.2.1 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32(1)(b) and 5 (1)(f) FLK, Section 7 EFF, Section 7 and 15  | [ ] Yes [ ] No |
|  | Does the organisation ensure, through technical and organisational measures, that e-mail does not contain identifiable health data when unencrypted channels are used? | 5.5.4 | A.13.2\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32(1)(b)EFF, Sections 7 and 15 | [ ] Yes [ ] No |
|  | Does the organisation implement logging when unencrypted channels are used, in order to ensure that rules are not broken? | 5.5.4 | A.13.2\*A.12.4\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32(1)(b)EFF, Sections 7 and 15 | [ ] Yes [ ] No |
|  | Does the organisation process rule breaches when unencrypted channels are used as breaches? | 5.5.4 | (A.10.1.1\*,A.16.1\* &A.7.2.3\*) |  |  | [ ] Yes [ ] No | PJL, Section 23 first paragraphHRL, Section 22EFF, Sections 7 and 15FLK, Section 8 | [ ] Yes [ ] No |
|  | When unencrypted channels are used, does the organisation assess whether the collective information in an SMS or e-mail could result in a breach of the duty of confidentiality? | 5.5.4 | A.8.1.3\*A.8.2.3\* |  |  | [ ] Yes [ ] No | PJL, Section 15HPL, Section 21GDPR, Article 9(2)(i)EFF, Sections 7 and 15 | [ ] Yes [ ] No |
|  | Are all technical equipment and applications that connect to the internet covered by the organisation's measures relating to information security and data protection, including in risk assessments, access management and procedures regarding use? | 5.5.5 | A.14.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32(1)(b)FLK, Sections 6, 7 and 8 | [ ] Yes [ ] No |
|  | Has the organisation implemented the following measures when connecting to the internet: * technical measures which help to prevent accidental disclosure and unauthorised access to personal health data?
* logging to verify that rules are not broken. Breaches of rules shall be handled as a breaches and personnel-related consequences shall be considered?
 | 5.5.5 | A.14.1.2\*A.15.1.3\*A.7.2.3\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Article 32(1)(b)EFF, Section 15FLK, Section 7 | [ ] Yes [ ] No |
|  | Does the organisation consider and determine the basis for processing in connection with digital communication with the data subject? | 5.6 |  |  |  | [ ] Yes [ ] No | GDPR, Articles 6 and 9 |  |
|  | Does the organisation assess suitable solutions and communication channels in connection with digital communication with the data subject? | 5.6 | A.13.2\*A.8.1.3\*A.8.2.3\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32EFF, Section 3 | [ ] Yes [ ] No |
|  | Does the organisation ensure that personal health data is not made available in such a way that patients/health care users are dependent on storing the data on their own equipment in order to familiarise themselves with the information? | 5.6 | A.13.2\*A.8.1.3\*A.8.2.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 25 | [ ] Yes [ ] No |
|  | Does the organisation ensure that procedures are established to ensure that messages to patients are not intrusive and do not violate privacy, while at the same time providing the patients with sufficient information? | 5.6 | A.8.1.3\*A.8.2.3\*8.2\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22EFF, Section 8 |  |
|  | Does the organisation implement sufficient measures to ensure that messages are sent to the correct recipient? | 5.6 | A.9.4.2\*A.13.2\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32 and 5 (1)(f)EFF, Section 8 | [ ] Yes [ ] No |
|  | Does the supplier ensure that controllers who use the supplier's products and services are able to fulfil statutory requirements and the requirements of the Code? | 5.7 | A.15.1.2 |  |  | [ ] Yes [ ] No | GDPR, Article 28FLK, Section 7 | [ ] Yes [ ] No |
|  | Does the supplier ensure that it has procedures in place which impose a duty of confidentiality on all employees concerning personal health data and other confidential information? | 5.7.1 | (A.15.1.2\*&A.13.2.4\*) |  |  | [ ] Yes [ ] No | PJL, Section 15HPL, Section 21GDPR, Article 5(1)(f) and 32 | [ ] Yes [ ] No |
|  | Is the controller ensured access to the supplier’s confidentiality declarations if necessary? | 5.7.1 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 |  |
|  | In connection with the provision of services or the delivery of hardware, systems, etc, have the security requirements that must be met in order for the controller to fulfil its responsibilities been agreed in writing with suppliers? | 5.7.2 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 | [ ] Yes [ ] No |
|  | Do the agreements include obligations which require the parties to fulfil the requirements and measures that follow from the Code for information security in force at any one time, as well as regulations concerning sanctions in the event of a breach of the Code and the agreement in general? | 5.7.2 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Articles 28 and 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Does the organisation ensure, through relevant agreements, that the supplier has satisfactory internal control in place with regard to security audits and breaches management? | 5.7.2 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 |  |
|  | In the event of the contracting out of services (outsourcing) covering ICT functions or other functions of significance to information security or data protection, does the agreement cover at least cover the following points:* documented risk assessment which demonstrates that the level of risk to which the outsourcing organisation is exposed is acceptable and that the level of security stipulated in the Code has been established. When outsourcing ICT services to other countries, the circumstances in the host country should be assessed because they may impact on the risk assessment.
* the tasks that are of significance to security which are covered, and the responsibility for such tasks
* description of the supplier's solution and interface with respect to the organisation in the form of a configuration map
 | 5.7.3 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 |  |
|  | Does the agreement ensure that the organisation is also granted the right to audit the supplier's activities relating to the agreement? | 5.7.3 | A.15.1.2 |  |  | [ ] Yes [ ] No | GDPR, Article 28 |  |
|  | Does the organisation have an appropriate plan in place to safeguard information security and data protection upon conclusion of the service delivery? | 5.7.3 | A.15.2.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 28 and 32PJL, Section 22HRL, Section 21 |  |
|  | In connection with the outsourcing of services, has it been agreed that, upon termination of the contract, a signed declaration shall be provided by the supplier confirming that all data belonging to the organisation has been returned or erased by the agreed time? | 5.7.3 | A.15.1.2\*A.15.2.2\*A.8.1.4\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 |  |
|  | Has it been agreed that the processor shall only process personal health data in accordance with instructions from the controller? | 5.7.4 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 and 29 |  |
|  | Does the agreement stipulate how the processor may process data on behalf of the controller? | 5.7.4 | A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28(3) |  |
|  | Does the agreement stipulate that the controller may only use processors who provide adequate guarantees that they will implement appropriate technical and organisational measures which ensure that the processing fulfils the requirements of the Personal Data Act? | 5.7.4 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 |  |
|  | Does the agreement stipulate that the processor shall not engage subcontractors without the prior specific or general permission of the controller?  | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 28(2) |  |
|  | Does the agreement stipulate that, if general, written permission is obtained, the processor shall notify the controller of any plans to substitute subcontractors? | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 28(4) |  |
|  | Does the agreement with the supplier stipulate that subcontractors are subject to the same obligations as the processor under the processor agreement? | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 28(4) |  |
|  | Has it been agreed that the agreement between the supplier and the subcontractor may be made available to the controller? | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 |  |
|  | Has the processor agreement been established in writing? | 5.7.4.2 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 28(3) |  |
|  | Does the agreement state that the processor undertakes to fulfil statutory requirements and the requirements of the Code? | 5.7.4.2 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 |  |
|  | Does the processor maintain an overview (record) of all categories of processing activities that are carried out on behalf of a controller? | 5.7.4.3 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Yes [ ] No | GDPR, Article 30(2) | [ ] Yes [ ] No |
|  | Does the controller ensure that the processor receives the information necessary to enable the processor to obtain such an overview? | 5.7.4.3 | A.15.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 28 and 30 |  |
|  | If the processor processes personal health data from a number of organisations, has the processor implemented technical measures which cannot be overridden by users to ensure that barriers are established between the organisations in accordance with the completed risk assessment? | 5.7.4.4 | A.9.1\*A.9.2\*8.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 28 and 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Does the processor notify the controller without delay of any breaches relating to data protection security? | 5.7.4.4 | A.16.1\* |  |  | [ ] Yes [ ] No | GDPR, Article 33(2) | [ ] Yes [ ] No |
|  | Through an agreement concerning maintenance, remote access and physical service, has the organisation ensured that:* the supplier’s equipment that is used for an online connection via a communication network or supplied equipped which is connected to the organisation’s equipment has no malware which contains viruses, etc. and that the equipment is protected against access by unauthorised parties
* all access and physical access shall be authorised by the organisation. Access shall be logged and controlled
* availability of personal health data shall insofar as is possible be maintained when the supplier performs work on the organisation’s equipment/software
 | 5.7.5 | A.15.1.2\*A.6.2.2\*A.11.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 28 and 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Do organisations in the healthcare and care services sector which use information systems that process personal health data require built-in data protection in the solutions? | 5.7.6 | A.14.1.1\*A.14.2\*A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 25EFF, Section 15 |  |
|  | Do the information systems have functionality that meets statutory and relevant requirements in the Code? | 5.7.6 | A.14.1.1\*A.14.2\*A.15.1.2\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21EFF, Section 15 |  |
|  | Are procurement, supplier follow-up and supplier management covered by the organisation’s information security management system?All phases of supplier management, from procurement to conclusion of the agreement, shall be covered. | 5.7.7 | A.15.1 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 28EFF, Section 15 |  |
|  | Does the organisation ensure supplier follow-up through:* clarity regarding responsibilities and roles
* ensuring that specialist resources within information security and data protection participate in procurements and supplier management
* ensuring that the organisation’s management (and the board if relevant) are normally involved in decisions concerning the use of private suppliers and/or the outsourcing of services with a certain scope
 | 5.7.7 | A.15.1\*A.6.1.1\*7.2\*5.1\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 28EFF, Section 15 |  |
|  | Is the establishment of requirements and necessary security measures in connection with the use of suppliers based on a comprehensive risk assessment? | 5.7.7 | A.14.1.1\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32 |  |
|  | Do risk assessments in connection with the use of suppliers always encompass scenarios that include the supplier's authorised and, where applicable, unauthorised access to personal health data and other confidential information? | 5.7.7 | A.15.1.1\*A.8.2\*8.2\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32 |  |
|  | Is it ensured that relevant security requirements are included in all procurements? | 5.7.7 | A.14.1.1 |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32FLK, Section 7 |  |
|  | Does the organisation ensure that it has sufficient client expertise at its disposal? | 5.7.7 | 7.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 32 |  |
|  | Do organisations which transfer personal data to other countries ensure that the level of protection stipulated in the Personal Data Act is not undermined through the transfer? | 5.7.8 | A.13.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 45 | [ ] Yes [ ] No |
|  | When the organisation transfers personal data to states outside the EU/EEA, known as “third countries”, does it use one of the grounds for transfer stipulated in the Regulation? | 5.7.8 |  |  |  | [ ] Yes [ ] No | GDPR, Articles 45, 46 and 47 |  |
|  | When transferring data to countries outside the EU/EEA, does the organisation have sufficient expertise (e.g. legal expertise) at its disposal in order to implement this in accordance with applicable requirements? | 5.7.8 | 7.2\* |  |  | [ ] Yes [ ] No | GDPR, Article 32 |  |
|  | Does the controller carry out comprehensive risk assessments in connection with the use of cloud services and otherwise follow the requirements for agreements and supplier monitoring stipulated in the Code? | 5.7.9 | A.15.1\*A.15.2\*8.2\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32 and 35FLK, Section 6 |  |
|  | Are the following points safeguarded in connection with the use of cloud services:* the distribution of responsibility between the controller and the processor has been clarified, and adapted to the delivery model being used
* the controller has an overview of where data is processed geographically, so that the requirements of section 5.7.8 can be addressed
* the controller shall ensure that any standard agreements that the cloud provider may have are not in breach of applicable statutory requirements and the requirements of the Code
* the controller shall have an appropriate plan in place to safeguard information security and data protection upon conclusion of the cloud service
 | 5.7.9 | A.15.1\*A.15.2\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 28 and 32 |  |
|  | Are incidents (such as breaches of procedures, data protection or information security) treated as a breach? | 5.8.1 | A.16.1.4\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 33 | [ ] Yes [ ] No |
|  | Are breaches processed in order to restore the normal state, eliminate the cause of the breaches and prevent repetition? | 5.8.1 | (10.1\*,A.16.1.5\*&A.16.1.6\*) |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 32  | [ ] Yes [ ] No |
|  | Does the organisation have procedures in place for detecting and managing breaches? | 5.8.1 | A.16.1.1 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 5(2) and 32FLK, Section 7 and 8 | [ ] Yes [ ] No |
|  | Is the processing of breaches documented? | 5.8.1 | A.16.1 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Article 33 (5) | [ ] Yes [ ] No |
|  | Does the organisation collect factual information concerning the sequence of events to enable corrective measures to be established? | 5.8.1 | A.16.1 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22 | [ ] Yes [ ] No |
|  | Are the effects of corrective measures assessed, and are any other measures implemented as and when necessary? | 5.8.1 | 10.1A.16.1.6 |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22 | [ ] Yes [ ] No |
|  | In the event of serious or repeated breaces, is a new risk assessment carried out? | 5.8.1 | 10.1\*10.2\*8.2\* |  |  | [ ] Yes [ ] No | PJL, Section 23HRL, Section 22GDPR, Articles 24 and 32 | [ ] Yes [ ] No |
|  | Are breaches reports containing personal data or information of importance to information security secured? | 5.8.1 | A.13.2.1 |  |  | [ ] Yes [ ] No | GDPR, Articles 32 and 5(1)(f) | [ ] Yes [ ] No |
|  | If a breaches constitutes a breach of personal data security and has resulted, or will result, in a medium or high risk for the data subject, will the controller report the breaches to the Norwegian Data Protection Authority within 72 hours?  | 5.8.2.1 | A.16.1\* |  |  | [ ] Yes [ ] No | GDPR, Article 33 |  |
|  | Will the data subject be notified of the breaches if it is likely that the breaches will entail a high level of risk for the data subjects (patients/users)?  | 5.8.2.2 | A.16.1\* |  |  | [ ] Yes [ ] No | PJF, Section 14 third paragraphGDPR, Article 34 |  |
|  | Does the organisation provide data subjects with at least the following information:* Description of the breach
* Name and contact details for the data protection officer or other point of contact where more information may be obtained
* Description of the likely consequences of the breaches
* Description of the measures that the organisation has implemented or is proposing to implement in order to manage the breach, including (where relevant) measures to reduce any harmful effects of the breach
 | 5.8.2.2 | A.16.1\* |  |  | [ ] Yes [ ] No | GDPR, Articles 33 and 34 |  |
|  | Do organisations that provide healthcare and care services notify the Norwegian Board of Health Supervision of any breaches arising from errors and breaches in information systems?The duty of notification shall be triggered: * in the event of death or very serious injury to a patient or healthcare user
* as a result of the provision of healthcare and care services
* when the outcome is unexpected based on foreseeable risks
 | 5.8.3 | A.16.1\* |  |  | [ ] Yes [ ] No | HTIL, Section 6HTL, Section 12-3 a |  |
|  | Does the organisation ensure the following in connection with incidents which result in notification of the Norwegian Board of Health Supervision:* follow up and inform patients and relatives
* review the incident
* identify and follow up risk mitigation measures
 |  | A.16.1\* |  |  | [ ] Yes [ ] No | PBL, Section 3-1 to 3-6 |  |
|  | Does the organisation ensure that the necessary personal health data is available? | 5.9 | A.17.1\*A.17.2\* |  |  | [ ] Yes [ ] No | PJL, Section 19GDPR, Article 32 (1) (b and c) | [ ] Yes [ ] No |
|  | Has the organisation mapped the consequences of non-availability in order to be able to establish emergency procedures to safeguard availability?The mapping shall be assessed for both the organisation and its authorised users. | 5.9 | A.17.1  |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | Are systems classified according to the following prioritisation: * Systems where the non-availability of a service could be critical, e.g.
	+ life-threatening for a patient
	+ critical for the organisation’s operation
* Systems where the non-availability of a service could have severe consequences, such as:
	+ increased risk of treating patients incorrectly
	+ deferment of medical investigations and treatment which could impact on life or health
	+ considerable additional work for personnel
	+ lost revenue for the organisation
* Systems where the non-availability of a service could have moderate consequences, such as:
	+ delays to medical investigations and treatment without any serious health consequences
	+ some additional work for personnel
	+ lost revenue for the organisation
	+ decreased reputation
	+ reduced confidence
	+ loss of efficiency
* Systems where protracted non-availability could be accepted
* Low priority systems
 | 5.9 | A.17.1\* |  |  | [ ] Yes [ ] No | PJL, Section 19 first paragraph and Section 22HRL, Section 21GDPR, Section 32 | [ ] Yes [ ] No |
|  | Is a review also carried out to determine which other systems and infrastructure the classified systems are dependent on?These shall have the same classification and acceptable level of risk as the classified systems. | 5.9 | A.17.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21 | [ ] Yes [ ] No |
|  | For each classification, has the management determined an acceptable level of risk for availability, in the form of at least a maximum period of non-availability?  | 5.9 | A.17.1\* |  |  | [ ] Yes [ ] No | PJL, Section 22HRL, Section 21GDPR, Section 32FLK, Section 6 |  |
|  | Has the organisation established emergency procedures based on the classification of the information systems for:* Alternative operation without the use of the information systems
* Alternative operation with partial support from the information systems
 | 5.9 | A.17.1\* |  |  | [ ] Yes [ ] No | PJL, Section 19 first paragraph, and Sections 22 and 23HRL, Sections 21 and 22FLK, Section 7 | [ ] Yes [ ] No |
|  | Are the emergency procedures practised, tested, revised and updated at least once a year? | 5.9 | A.17.1\* |  |  | [ ] Yes [ ] No | GDPR, Section 32PJL, Section 22HRL, Section 21FLK, Section 8 | [ ] Yes [ ] No |