



Ephorte Saksnummer 2023/806

og

Avtalenummer **xxxxxxx**

Bilag til SSA-K for

**Fosterovervåkning for levering til
Helseforetakene i Helse Vest**

SSA- K Bilag 3 Kundens tekniske plattform

Sist oppdatert: **29.06.2023**

Innhold

1	Innledning	4
1.1	Mål 4	
1.1.1	Konfidensialitet	4
1.1.2	Tilgjengelighet og integritet	4
1.1.3	Risiko	4
1.1.4	Personvern	4
1.2	Kilder til sikkerhetskrav.....	4
2	Omfang	5
3	Begrep og definisjoner	5
4	Autentisering	6
4.1	Brukerautentisering	6
4.2	Autentisering av utstyr	7
4.3	Autentisering av eksterne brukere	7
4.4	Single sign-on	7
4.5	Fler faktor autentisering	7
4.6	Automatisk time-out.....	7
4.7	Standarder and teknologi	7
4.7.1	Active Directory Autentisering	7
4.7.2	Integrert Windows Autentisering (IWA)	7
4.7.3	OpenID Connect	7
4.7.4	ID-Porten	8
4.7.5	HelseID	8
4.7.6	Azure AD Autentisering	8
5	Tilgangskontroll	8
5.1	Autorisasjon	8
5.2	Nødrettstilgang	8
5.3	Brukerroller	8
5.4	Fjerntilgang	8
5.5	Standarder og teknologi	9
5.5.1	Active Directory Sikkerhetsgrupper	9
5.5.2	XACML – attributtbasert tilgangskontroll	9
5.5.3	OAuth 2.0 / Azure AD	9
6	Operativ sikkerhet	9
6.1	Monitorering.....	9
6.1.1	Sentralisert hendelse logging og respons	10

6.2	Brukernavn og passord	10
6.3	Domenesikkerhet.....	10
6.4	Sikkerhetsoppdateringer og patcher	10
7	Kryptering	10
7.1	Ende-til-ende kryptering.....	10
7.2	Transportkryptering.....	11
7.2.1	TLS-protokoller	11
7.2.2	Anbefalte cipher suiter	11
7.3	Kryptering av lagrede data.....	11
7.3.1	Krypteringsstyrke	11
7.4	Sertifikater	12
7.4.1	Sertifikat nøkkellengde og avtrykk	12
7.5	Nøkkelhåndtering	12
7.5.1	Lagring av nøkler	12
8	Utvikling og testing	12
8.1	Programvareutvikling med innebygd personvern	12
8.2	Akseptansetesting.....	12
9	Compliance	13
9.1	Samsvar med lovverket.....	13
9.1.1	Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen)	13
9.1.2	Personvern og beskyttelse av personlig identifiserbar informasjon	13
9.2	Revisjon av informasjonssikkerhet	13
9.2.1	Oppfyllelse av sikkerhetspolicys og krav	13
9.2.2	Revisjon av tekniske tiltak	13
10	References	14
1	14	

1 Innledning

Helse Vests hovedoppgaver er pasientomsorg, helsetjenester, forskning, opplæring av pasienter og pårørende, utvikling av medisinsk praksis, omsorg og kompetanseutvikling og samarbeid med kommuner og fylkeskommuner.

For å oppfylle sine forpliktelser må Helse Vest behandle helse- og personopplysninger - relatert til helsevesen, statistikk og rapportering og i forskningsprosjekter. Denne informasjonen er i elektronisk form og må beskyttes. I tillegg behandler Helse Vest personlig informasjon om ansatte og kontaktpersoner innen partnerorganisasjoner.

Helse Vest er ansvarlig for all behandling av helse- og personopplysninger i informasjonssystemer og er databehandler for helseinformasjon for helseforetakene i regionen.

Helse Vest er underlagt bestemmelsene i helseloven, helseregisterloven, personopplysningsloven og Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten [1]. Loven stiller strenge krav til behandling av helse- og personopplysninger, for eksempel:

- Krav til tilgangskontroll for informasjon som er nødvendig for bruk i omsorg,
- Krav på at informasjonen skal være korrekt og oppdatert
- Bestemmelser om konfidensialitet

Helse Vest behandler helse- og personinformasjon i samsvar med alle relevante lover og forskrifter, herunder å sikre tilfredsstillende konfidensialitet, tilgjengelighet, integritet og kvalitet på informasjonen.

1.1 Mål

1.1.1 Konfidensialitet

Personvern og beskyttelse av helseinformasjon er en grunnleggende pasientrettighet og en forutsetning for tillit mellom pasienten og helseforetaket og den enkelte helsearbeideren. Tilfredsstillende konfidensialitet har derfor høy prioritet blant sikkerhetskravene.

1.1.2 Tilgjengelighet og integritet

Tilgang til relevant og nødvendig helse- og personinformasjon er en forutsetning for å gi god helsehjelp. Tilfredsstillende sikkerhet for tilgjengelighet og integritet kan være viktig og må prioriteres høyere enn behovet for konfidensialitet

1.1.3 Risiko

Helse Vest IKT aksepterer ikke brudd på sikkerhetsinstruks, datainnbrudd eller andre negative hendelser knyttet til informasjonssikkerhet. Tiltak er innført for å senke risiko for at negative hendelser, selv med moderat sannsynlighet, ikke skal skje. Sikkerhetstiltakene må ikke omgå hverken av ansatte eller eksterne.

1.1.4 Personvern

Helse Vest behandler bare personinformasjon når det er nødvendig for å yte helsehjelp. Pasienter må gi samtykke til behandlingen av helse- og personinformasjon når ikke tilgang til informasjon er lovbestemt.

Informasjonen som behandles må ha nødvendig kvalitet for å kunne benyttes til formålet. Alle som etterspør data vil motta generell informasjon om helseforetakets regler for behandling av person- og helseinformasjon. Pasienter/personer som er registrert har også rett til tilgang til informasjonen og vil kunne få eventuelle feil korrigert.

1.2 Kilder til sikkerhetskrav

De primære kildene til sikkerhetskrav:

- Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) [1]
- Helse 2035 [2]
- Helse Vest Information Security Management System [3]
- Nasjonal Sikkerhetsmyndighet – Grunnprinsipper for IKT-sikkerhet [4]
- ISO 27002:2013 [5]

2 Omfang

Formålet med dette dokumentet er å komplettere kravspesifikasjoner for innkjøp av informasjonssystemer til bruk i Helse Vest. Dokumentet oppsummerer obligatoriske krav og opsjoner for informasjonssikkerhet basert på kildene listet i kap. 1.2.

3 Begrep og definisjoner

Term/Definition	Description
AD	Microsoft Active Directory
AAD	Azure Active Directory
MAC Address	En media access control address (MAC-adresse) til en enhet er en unik identifikator tilordnet nettverksgrensesnitt for kommunikasjon ved datalinklaget i et nettverkssegment
SSO	Single sign-on (SSO) er en egenskap for autentisering mot flere relaterte, men uavhengige programvaresystemer. Med denne egenskapen logger en bruker seg på med en enkelt brukerID og passord for å få tilgang til et tilkoblet system eller systemer uten å bruke forskjellige brukernavn eller passord, eller i noen konfigurasjoner på en sømløs måte logge på i hvert system.
OpenID Connect	OpenID Connect (OIDC) er et autentiseringslag på toppen av OAuth 2.0, et autorisasjonsrammeverk. Standarden er kontrollert av OpenID Foundation.
Key Distribution Center	I kryptografi er et nøkkel distribusjonssenter (KDC) en del av et kryptosystem som er ment å redusere risikoen som ligger i utveksling av nøkler.
RBAC	Role-based-access-control (RBAC) er en policy-nøytral tilgangskontrollmekanisme definert rundt roller og privilegier. Komponentene i RBAC som

	rolletillatelser, brukerrolle og rolle-rolleforhold gjør det enkelt å tilordne brukeroppgaver.
XACML	XACML står for "eXtensible Access Control Markup Language". Standarden definerer et deklarativt finkornet, attribusjonsbasert tilgangskontrollpolitisk språk, en arkitektur og en behandlingsmodell som beskriver hvordan du skal evaluere tilgangsforespørsler i henhold til reglene definert i policyer.
ABAC	Attribusbasert tilgangskontroll (ABAC) definerer et tilgangskontrollparadigme der tilgangsrettigheter tildeles brukere gjennom bruk av policyer som kombinerer attributter sammen.
SIEM	Security Information and Event Management er et system for sikkerhet og hendelseshåndtering.
SOAR	Security Orchestration, Automation, and Response er et sikkerhetsorkestrerings-, og automatiserings- og responssystem
Transport Layer Security (TLS)	Transport Layer Security (TLS) og forgjengeren, Secure Sockets Layer (SSL), er kryptografiske protokoller som gir kommunikasjonssikkerhet over et datanettverk.
AES	Advanced Encryption Standard (AES), også kjent med sitt opprinnelige navn Rijndael, er en spesifisering for kryptering av elektroniske data etablert av U.S. National Institute of Standards and Technology (NIST) i 2001. AES er basert på et designprinsipp kjent som et substitusjons-permutasjonsnettverk, en kombinasjon av både substitusjon og permutasjon, og er raskt i både programvare og maskinvare.
HL7 FHIR	FHIR® - Fast Healthcare Interoperability Resources (hl7.org/fhir) - er en neste generasjons standardrammeverk laget av HL7.

4 Autentisering

4.1 Brukerautentisering

Brukere må autentiseres mot katalogtjenesten i Helse Vest, Microsoft Active Directory (AD). Løsningen bør støtte både brukernavn/passord og smartkortautentisering. Brukeren kan også automatisk autentiseres dersom løsningen støtter single sign-on.

4.2 Autentisering av utstyr

Utstyr som skal kobles på Helse Vests nettverk må godkjennes før tilkobling. Utstyres MAC adresse blir koblet mot en IP adresse eller et godkjent sertifikat i Helse Vest benyttes.

4.3 Autentisering av eksterne brukere

Brukere som trenger tilgang til systemer fra en ekstern lokasjon må autentisere sin identitet ved bruk av 2-faktor autentisering. All ekstern tilgang til systemer i Helse Vest må risiko vurderes og godkjennes før bruk.

4.4 Single sign-on

Helse Vest benytter Microsoft infrastruktur for Identitets og tilgangsstyring. Single Sign-On (SSO) skal støttes på applikasjonslaget ved hjelp av protokollen OpenID Connect som beskrevet i kapittel 4.7.3. Denne vil også kunne gi SSO mot HelseID [6].

4.5 Fler faktor autentisering

Flerfaktorautentisering (MFA) er et ekstra sikkerhetslag for bruker kontoen. Når den er aktivert, må du oppgi passordet ditt og deretter godkjenne innloggingsforsøket med en spesiell app, tidssensitiv kode eller en annen kode enhet. Helse vest benytter RSA og Azure AD som løsninger for fler faktor autentisering. Brukere som trenger tilgang til systemer fra en ekstern lokasjon må autentisere sin identitet ved bruk av 2-faktor autentisering. Brukere med tilgang til eksterne systemer (skytjenester) må autentisere sin identitet ved bruk av fler faktor autentisering. All ekstern tilgang til systemer og eksterne systemer i Helse Vest må risiko vurderes og godkjennes før bruk.

4.6 Automatisk time-out

Inaktive brukere skal logges ut av løsningen automatisk. Time-out skal kunne konfigureres for grupper, lokasjoner og klientenheter.

4.7 Standarder and teknologi

4.7.1 Active Directory Autentisering

Active Directory-godkjenning lar brukere logge seg på systemet hvis de har en konto i et Active Directory-domenet. Ved å bruke Kerberos autentiseringsprotokoll kan applikasjonen autentisere enhver bruker sikkert mot Helse Vest-domenet. Systemet bruker Kerberos-protokollen for å sjekke brukerens hovednavn og passord mot et Key Distribution Center (KDC) for domenet.

4.7.2 Integrert Windows Autentisering (IWA)

Integrert Windows Autentisering ber ikke brukeren om brukernavn og passord. Informasjon om Windows-brukerkontoen på klientdatamaskinen brukes til godkjenning. Men hvis autentiseringsutvekslingen ikke identifiserer brukeren, ber nettleseren brukeren om autentiseringsinformasjon. Når du aktiverer integrert Windows Autentisering initierer applikasjonen en kryptografisk utveksling med webserveren ved å bruke enten NTLM eller Kerberos-godkjenning for å validere brukeren.

4.7.3 OpenID Connect

OpenID Connect er (OIDC) en åpen standard som er plassert på toppen av OAuth 2.0-protokollen. Det gjør det mulig for klienter å bekrefte identiteten til sluttbrukeren basert på autentiseringen utført av en autorisasjonsserver, samt å få grunnleggende profilinformasjon om sluttbrukeren på en interoperabel og REST-lignende måte. Helse Vest støtter denne protokollen for autentisering og enkeltpålogging ved å bruke Microsoft Azure AD (AAD).

4.7.4 ID-Porten

ID-porten er en offentlig autentiseringsløsning for offentlige tjenester. Ved å autentisere mot ID-porten kan du potensielt få tilgang til mer enn 1000 forskjellige tjenester fra offentlige etater. ID-porten støtter forskjellige elektroniske ID-er: MinID, BankID, BankID på mobil, Buypass eller Commfides. Helse Vest kan bruke ID-porten for tjenester overfor publikum.

En implementeringsveiledning for ID-porten er publisert på [GitHub](#).

4.7.5 HelseID

HelseID [6] er en felles påloggingsløsning for helse- og omsorgssektoren. Den legger til rette for at helsepersonell kan få engangspålogging med én elektronisk ID (e-ID) i hele helsetjenesten, og for at sektoren lettere kan dele data og dokumenter. HelseID benytter OpenID Connect som beskrevet i kapittel 4.7.3.

4.7.6 Azure AD Autentisering

Helse Vests brukere er synkronisert til Azure AD (AAD) der de kan autentisere seg for å benytte skytjenester. Azure støtter moderne autentiseringsprotokoller som OpenID Connect beskrevet i kapittel 4.7.3.

5 Tilgangskontroll

Når bruker er autentisert, må det være mekanismer som regulerer tilgangen til systemet, utstyret eller dataene. Disse mekanismene skal også regulere rettighetene til hva brukere kan utføre med utstyret eller med dataene.

5.1 Autorisasjon

Tilgangen skal gis med rettigheter til å lese, registrere, redigere og korrigere helseopplysninger. Autorisasjon for tilgang kan bare gis når det kreves for helsehjelp basert på tjenstlig behov og under taushetsplikt.

5.2 Nødrettstilgang

I en nødsituasjon kan autoriserte brukere gi seg tilgang til helseinformasjon. Årsakene til nødrettstilgangen må dokumenteres og logges av informasjonssystemet.

Tilgangen vil bli fulgt opp som et avvik. Hvis pasientens tilstand er alvorlig, kan nødrettstilgang også brukes til å vise informasjon som er sperret mot tilgang.

5.3 Brukerroller

Tydelig definerte roller og rollemaler er gode verktøy for å definere tilgangsrettigheter i et helserelatert system. Fullmakt til å skrive, slette, lese og redigere og på annen måte behandle data på skal gis i den grad det er nødvendig for å utføre jobben for den enkelte. Denne autorisasjonen bør gis på gruppenivå, slik at det er lett for andre å gå inn i samme rolle. Granulariteten til roller er gitt av informasjonssystemets art og antall brukere.

5.4 Fjerntilgang

Tilgang for fjern administrasjon av servere og systemer er kun tillatt via Helse Vest sin løsning for fjerntilgang. Alle med tilganger til servere eller systemer må ha egne individuelle kontoer som har begrenset rettigheter i.h.t. dokumentert behov.

5.5 Standarder og teknologi

5.5.1 Active Directory Sikkerhetsgrupper

Sikkerhetsgrupper i Helse Vest Active Directory brukes til å kontrollere tilgang til systemer og andre ressurser innen domenet. Role Based Access Control (RBAC) i informasjonssystemer implementeres ved hjelp av sikkerhetsgrupper for tilordning av tillatelser for en gitt gruppe av systembrukere.

Systemet må lese tillatelser fra Active Directory og utføre dem på systemnivå for alle autentiserte brukere.

5.5.2 XACML – attributtbasert tilgangskontroll

Helse Vest bruker en sentralisert autorisasjonstjeneste som utnytter XACML-standard "eXtensible Access Control Markup Language". Tjenesten mottar attributter fra forespørrere og gjør oppslag mot informasjonsskilder for ytterligere attributter. En beslutning om tilgang blir tatt i henhold til gitte policyer der attributtene inngår.

Autorisasjonstjenesten brukes først og fremst når informasjonssystemer trenger å sikre at en bruker har tilgang til en beskyttet ressurs, for eksempel en pasientjournal, og trenger en dynamisk beslutningsmodell.

5.5.3 OAuth 2.0 / Azure AD

OAuth 2.0 er en åpen standard for autorisering. Helse Vest benytter Azure AD som benytter OAuth 2.0 for autorisering. Azure AD benytter også Role Based Access Control (RBAC) for brukere, grupper eller service kontoer.

6 Operativ sikkerhet

6.1 Monitorering

Systemet må kunne logge hendelser. Informasjonselementer som er inkludert i loggen skal kunne konfigureres i systemet. Beskrivelsen av hendelsene må være nøyaktig og tydelig. Hensikten med overvåking av hendelser er:

- Dokumentere uønskede hendelser
 - Identifisere hendelsen
 - Er det et problem? (Flere forekomster av samme hendelse)
 - Rettelse
 - Dokumentasjon av hendelse og handling.
 - Pasientsikkerhet
 - Revisjon
 - Overholdelse av lover og regler

Som et minimum skal følgende logges for tilgang til helse- og personopplysninger:

- PC-navn
- Unik BrukerID
- Aktiv brukerrolle
- Brukerens helseforetak
- Brukerens organisasjonsenhet (avdeling eller seksjon)
- Informasjonselementene brukeren har fått tilgang til
- Dato og tid
- Beskrivelse av handlingen

- Årsak til nødrettstilgang
- Forsøk på å få uautorisert tilgang
- Når du får tilgang til informasjon på tvers av organisasjonsgrenser, må følgende logges for begge organisasjoner:
 - BrukerID og brukerorganisasjon (helseforetak og avdeling / org. enhet)
 - Årsak til bruk
 - Tid og dato

6.1.1 Sentralisert hendelse logging og respons

Microsoft Sentinel er en skalerbar skytjeneste for sikkerhetsinformasjon og hendelseshåndtering (SIEM), og et sikkerhetsorkestrerings-, og automatiserings- og responssystem (SOAR) løsning. Skytjenester som skal benyttes i Helse Vest bør ha mulighet for å videresende sikkerhets relaterte hendelses logger til Microsoft Sentinel.

6.2 Brukernavn og passord

Systemet må overholde Helse Vest IKT-standard for brukere og passord for servere.

Helse Vest IKTs standard for serverbrukere og passord:

- Lokale brukere brukes ikke til driftsformål
- Brukere av domener eller tjenester må brukes
- Krav til spesifikke navn på brukere er ikke tillatt
- Krav til spesifikke passord er ikke tillatt
- Passord må periodisk endres

6.3 Domenesikkerhet

Microsoft-servere må være medlemmer av Helse Vests domene og kjøres under standard domenesikkerhetsinnstillinger. Serverne må kjøre antivirusprogramvare og skanning i sanntid, og løsningen må støtte disse sikkerhetskontrollene.

Hvis den foreslåtte løsningen ikke kan bruke standard sikkerhetsoppsett i Helse Vest, må leverandøren oppgi alle avvik og gi forslag til hvordan håndtere sikkerhetsoppsettet. Tredjepartsdrivere som skal installeres på servere, må være WHQL-godkjent (Windows Hardware Quality Labs-sertifisert).

6.4 Sikkerhetsoppdateringer og patcher

Alle servere og infrastrukturkomponenter tilknyttet systemet må oppdateres og patches regelmessig. Dette inkluderer operativsystemer, databasesystemer, applikasjonsservere og klienter.

Systemkomponenter installert på servere skal kunne håndtere sikkerhetsoppdateringer uten forhåndsgodkjenning fra leverandøren.

7 Kryptering

Kryptering skal brukes for å beskytte konfidensialitet, autentisitet og / eller integritet til informasjon.

7.1 Ende-til-ende kryptering

All datakommunikasjon som involverer helse- og personlig informasjon i nettverk utenfor Helse Vests-kontroll, må være kryptert. Dette gjelder imidlertid både i Helse Vests interne nettverk, internett og i

nettverket til tjenesteleverandøren. Tilsvarende må overføringen av helseinformasjon mellom leverandøren og eventuelle underleverandører sikres.

Kryptering fra ende til annen betyr at det ikke skal være et mellomtrinn der data blir lest eller lagret i "klartekst".

For krypteringskrav, se i følgende dokument: "Kravspesifikasjon for PKI i offentlig sektor" [7].

7.2 Transportkryptering

All kommunikasjon mellom systemer som involverer personlig informasjon, må være kryptert. Transport Layer Security (TLS) er mye brukt til dette formålet. TLS-protokollen skal gi konfidensialitet og dataintegritet mellom to kommuniserende systemer.

7.2.1 TLS-protokoller

Listen under angir anbefalte TLS-protokoller og TLS-protokoller som ikke skal benyttes

Prioritet	1.	TLS	1.3
Prioritet 2.	TLS 1.2		

TLS 1.1 og TLS 1.0 skal ikke benyttes. (SSL-protokoller skal ikke benyttes - SSL 3.0 og SSL 2.0)

7.2.2 Anbefalte cipher suiter

De anbefalte cipher suiteene i prioritert rekkefølge:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256

TLS 1.2:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0x00C02C)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0x00C030)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0x00C02B)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x00C02F)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0x00C024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0x00C028)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0x00C023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0x00C027)

7.3 Kryptering av lagrede data

For å forhindre uautorisert innsyn i personlig- eller pasientinformasjon, kan lagrede data også krypteres. Dette er et krav i tilfeller der sensitive data lagres midlertidig eller permanent i databaser eller filstrukturer der flere brukerroller med ulikt ansvar må ha tilgang.

7.3.1 Krypteringsstyrke

Programvare for krypterings- og dekryptering skal bruke en AES symmetrisk krypto-algoritme med en minste nøkkellengde på 256 biter.

For Secure Hash Algorithm anbefalers SHA-384/512 eller SHA3-384/512.

For RSA algoritmer anbefales en minste nøkkellengde på 3072 biter. Krypteringsmoduler skal følge FIPS 140-2 eller tilsvarende standard.

7.4 Sertifikater

Alle systemer som benytter transportkryptering skal benytte sertifikater fra godkjente utstedere. Helse Vest har også en intern PKI-løsning som kan benyttes for å utstede interne sertifikater.

7.4.1 Sertifikat nøkkellengde og avtrykk

Benytt elliptisk kurve-baserte sertifikater med minimum 256 bits nøkkellengde eller RSA-baserte sertifikater med minimum 3072 bits nøkkellengde. Benytt SHA-2-baserte avtrykk med minimum 256 bits lengde.

7.5 Nøkkelhåndtering

Sikker nøkkelhåndtering er vesentlig for konfidensialiteten i kryptert informasjon.

- Sikre konfidensialitet og autentisitet av hemmelig og offentlig nøkler, så vel som å sikre hemmelig og offentlige nøkler mot uautorisert bruk
- Sikre autentisitet av offentlige nøkler
- Sikre tilgjengelighet til hemmelig og offentlige nøkler.

7.5.1 Lagring av nøkler

Azure Key Vault er en sky-tjeneste for sikker lagring og tilgang til «hemmeligheter». En «hemmelighet» er alt som en ønsker å ha streng tilgangskontroll til, slik som API-nøkler, passord, sertifikater, eller kryptografiske nøkler. Helse Vest benytter Azure Key Vault og det anbefales å benytte denne funksjonaliteten for sikker oppbevaring av «hemmeligheter» spesielt for skytjenester og tjenester med ekstern tilgang (uten bruk av VPN).

8 Utvikling og testing

8.1 Programvareutvikling med innebygd personvern

Sikker utvikling er et krav for å bygge en sikker tjeneste, arkitektur, programvare og system. Datatilsynet har utviklet retningslinjer for å hjelpe organisasjoner med å forstå og oppfylle kravet om databeskyttelse ved design og som standard i artikkel 25 i den generelle personvernforordningen. Retningslinjene dekker faser gjennom hele livssyklusen for programvareutvikling: Opplæring, krav, design, koding, testing, release og vedlikehold [8].

8.2 Akseptansetesting

Akseptansetest skal omfatte testing av krav til informasjonssikkerhet og overholdelse av sikker systemutviklingspraksis, ref. kapittel **Feil! Fant ikke referanse-kilden..** Testing bør utføres på programvarekomponenter og integrerte systemer. Automatiserte verktøy kan benyttes, for eksempel verktøy for kodeanalyse eller sårbarhetsskannere, og skal verifisere retting av sikkerhetsrelaterte feil.

Testingen skal utføres i et realistisk testmiljø for å sikre at systemet ikke vil introdusere sårbarheter i organisasjonens miljø. Det skal ikke benyttes personinformasjon under testene.

Anonyme datasett eksisterer for testing med ekte pasient- og personinformasjon.

Løsningen skal kunne gjennomgå en penetrasjonstest i et produksjonslik miljø før den kan settes i produksjon.

9 Compliance

9.1 Samsvar med lovverket

9.1.1 Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen)

Normen er en bransjenorm for informasjonssikkerhet og personvern og utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren. Helse Vest er forpliktet til å oppfylle Normen [1] ved alle anskaffelser av informasjonssystemer.

9.1.2 Personvern og beskyttelse av personlig identifiserbar informasjon

EUs personvernforordning (GDPR) [9] vil gjelde for alle helseforetak i Helse Vest så vel som Helse Vest IKT. Programvareleverandører må utvikle systemer som bruker personvern ved design (ref. Kapittel 8.1) og systemtester som bekrefter at programvaren beskytter personopplysninger i samsvar med GDPR.

9.2 Revisjon av informasjonssikkerhet

Informasjonssystemer vil jevnlig bli gjenstand for revisjon for å sikre at organisasjonens retningslinjer og standarder for informasjonssikkerhet oppfylles.

9.2.1 Oppfyllelse av sikkerhetspolicies og krav

Systemet vil bli gjennomgått med hensyn på bruk og hva slags informasjon som behandles. Formålet med tilsynet er:

- Er bruk og behandling i samsvar med policies og krav?
- Genereres varsler hvis bruk og behandling avviker fra kravene?
- Blir varslene mottatt og behandlet?

9.2.2 Revisjon av tekniske tiltak

Systemets sikkerhetsmekanismer vil bli evaluert regelmessig. Formålet med tilsynet er:

- Er bruk og behandling i samsvar med de definerte kravene?
- Genereres varsler hvis bruk og behandling avviker fra kravene?
- Blir varslene mottatt og behandlet?

10 References

- [1] D. f. e-helse, «Norm for informasjonssikkerhet,» [Internett]. Available: <https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren>.
- [2] H. V. RHF, «Helse 2035,» 2017. [Internett]. Available: <https://helse-vest.no/Documents/Om%20oss/M%C3%A5l%20og%20strategiar/Helse2030/Helse2035%2007072017.pdf>.
- [3] H. V. ICT, «Styringssystem for Informasjonssikkerhet i Helse Vest,» 2012.
- [4] NSM, «Grunnprinsipper for IKT-sikkerhet,» [Internett]. Available: <https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt>.
- [5] I. O. f. Standardization(ISO), «ISO/IEC 27002:2013,» 2013. [Internett]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:en>.
- [6] N. Helsennett, «HelseID,» 2017. [Internett]. Available: <https://www.nhn.no/helseid/>.
- [7] a.-. o. k. Fornyings-, «Kravspesifikasjon for PKI i offentlig sektor,» [Internett]. Available: <https://www.regjeringen.no/link/ab5bc44e9cb84c19b250346d8ab5e904.aspx?id=2156639>.
- [8] Datatilsynet, «Software development with Data Protection by Design and by Default,» 2017. [Internett]. Available: <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/>.
- [9] E. D. P. Authorities, «The EU General Data Protection Regulation,» 2012. [Internett]. Available: <https://www.eugdpr.org/>.
- [10] a.-. o. k. Fornyings-, «Requirements specification for PKI in the public sector,» June 2010. [Internett]. Available: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/2010_kravspek_pki_engelsk.pdf?id=2156639.
- [11] D. f. e-helse, «The Code of Conduct for information security in the healthcare and care services,» 2016. [Internett]. Available: <https://ehelse.no/Documents/Normen/Engelsk/Code%20of%20Conduct%20v%205.2%20final.pdf>.
- [12] HL7, «HL7 FHIR AuditEvent,» 2017. [Internett]. Available: <https://www.hl7.org/fhir/auditevent.html>.