Frågor kopplat till lagring och hantering av forskningsdata

KTH19, forskare Skolan för teknikvetenskap

Datum: 230504

Fysiskt möte på KTH

Josefine Olsson, RiR

1. **Hur går bedömning av "känslighet" av data till?/Klassas information eller hur vet du hur då får hantera olika typer av forskningsdata?** Lagt till sedan jag skickade ut frågorna: Hanterar du "känslig" data? Har ni identifierat vad som är skyddsvärt.

Finns ett dokument om infoklassning på kth, ibland är han lite osäker på hur han ska tolka det.

"informationsklassificering KTH" = dokument, rubrik basnivå skydd. Han har skickat detta till mig.

Jobbar inte med några militära grejer och ingen kärnkraft. Däremot patientintegritet. Dels gdrp och dels patientdatalagen som måste följas – det mesta blir klass S1. Bilder från karolinska klass S2. CISO har sagt att det är ok. På de andra grundläggande – han menar R och T i dokumentet.

NN gör egna bedömningar men kan också fråga IT. Robin Roy dataskyddsombud och Patrik L pratar han med. Och numera pratar han med Rosa också.

Väldigt upp till NN sen att hantera det som tex S2 (han som forskningsledare är den som har koll på datan och de som jobbar under honom). Det som kth kan göra är att skriva styrdokument och rutiner. Väldigt mkt är delegerat till forskare och forskningsledare. Man får tänka själv helt enkelt. Vad kan hända om det kommer ut? Skrivs avtal om att något är hemligt? Samarbete med Karolinska.

X är pseudonymiserad (så som våra löneanalyser på Rir), bara metadata hur bilden är tagen exponeringsparametrar. Och tex nr 18 i serien och sen finns kodnyckel på karolinska vem personen är.

NN gör bedömning, är han osäker får han ta stöd av någon.

När delar med industrin – då ska de vara försiktiga, men de är lite mindre försiktiga, bara ett visst antal personer som får se den, använder då ändå kth:s system på ett mer normalt sett. Verkar inte lika känsligt som patientinfo.

Han tycker att det viktiga är hur man ska hantera den här datan – vad har kth förbundit sig till, finns ofta avtal att gå tillbaka till. Får använda sitt eget omdöme. Får hjälp av patrik L it-säkerhetschefen.

2. På vilken/vilka lagringsytor lagrar du forskningsdata?

Olika för olika forskningsdata.

Medicinska personuppgifter. Krypterade hårddiskar, antingen i någons laptop (då krypterad) inga anda har tillgång till. Backuper – ofta krypterad externdisk med få personer som har tillgång till.
Eller krypterad hårddisk på server – här finns mest känslig data (finns rutin för det som ska uppfylla ett antal åtkomstkrav) – finns en rutin för detta som NN och CISO tagit fram, kan fjärransluta – väldigt noga med säkerhetsregler.

Info som är konfidentiell men lägre skyddsvärde – tex funderar på att patentera eller tex från industrisamarbetspartner – då ska det finnas ett grundläggande åtkomstskydd, man kan ha det på sin dator och inte tillgänglig för andra datorer, lösenord på datorn och låser sina lokaler. Där tillåter molntjänster som kth tillhandahåller som tex onedrive. Kan skicka info på mail till varandra med folk som har rätt att få åtkomst till info. Däremot mailas inte röntgenbilder om de inte är helt anonymiserade.

Lite olika säkerhetsnivåer baserat på säkerhetsnivå. Man kan skriva långa dokument – men orkar folk läsa det? Bra med enkla dokument och kontinuerlig dialog med forskare menar han.

3. Vet du på vilka lagringsytor du får lagra forskningsdata utifrån klassning/"känslighet"?

Finns regler som de följer internt. Känner sig osäker på om det är i linje med personer högre upp på kth. Har inte pratat så mkt med CISO sen 2020. Nu gjorde NN samtal med Patrik och Rosa inför detta mötet idag och de verkade vara ok med detta.

4. Hur delar du med dig av forskningsdata till andra parter t.ex. andra forskare? (exempelvis via mail, usb-minne, annan lösning)

Mail skickar de inte personuppgifter genom.

USB-minne – kan flytta grejer på okrypterad hårddisk, pratar om att de undviker usb okrypterat, krypterat ok. Konfidentiella data mailar ganska mkt fram och tillbaka med företag tex.

Företag X och karolinska och kth samarbete mellan dessa parter: X delar info genom tjänst och om de säger att det är ok och då delar kth info med dem på samma sätt.

5. Delas forskningsdata genom digitala videomöten, exempelvis genom Teams eller annan lösning?

Tittar tex på bilder i Zoom, då har man koll på vilka som deltar i mötet. Använder KTH:s Zoom-lösning. Administrerad av kth eller av fler universitet i sverige, under sveriges kontroll iaf.

Använder också teams med samarbetspartners som X. Om de startar mötet och vill att kth ska dela bild gör de det för då säger de att det är ok.

Undviker skicka fil med zoom, däremot att ta upp de på zoom är en förutsättning att kunna arbeta.

Handlar mest om att personen i andra änden har rätt att se infon.

6. **Hur vet du att du hanterar forskningsdata på ett korrekt sätt (främst utifrån konfidentialitet)? (finns t.ex. tydliga riktlinjer eller liknande från lärosätet att följa vad gäller klassning av information och lagring av data?)**

Han tycker inte att det är jättetydligt. Han skickar som sagt ett dokument till mig angående klassning. Det ger dock inte info om vart tex S2 – data får lagras.

Finns policy för egenadministrerade system. Egenadministrerade system är vad NN använder.

NN tycker att det är lite luddigt hur man ska översätta klassningen typ S2 till faktiska säkerhetsregler. Också frågan om det går att skriva för det finns så mkt olika forskning. Då handlar det mer om, om det tex finns avtal med regler då följer man de reglerna. Vissa avtal är jättetydliga och i vissa står det bara att info ska hanteras konfidentiellt och då får han mer använda sitt omdöme.

NN visar avtal med karolinska. Regler för en specifik datamängd – väldigt tydligt vad som gäller. NN skrev detta ihop med dataskyddsombud och CISO Han fick inte så mkt stöd av riktlinjer och så tycker han (från lärosätet).

7. **Följer lärosätet upp att du hanterar forskningsdata på ett korrekt sätt (främst utifrån konfidentialitet)? I så fall hur?**

När NN var ny pratade han en del med dataskyddsombud och IT patrik L. men sen har han inte gjort det.

NN har inte haft någon kontakt om informationssäkerhet med dem efter det.

Inför detta möte med mig pratade han lite med dem samt Rosa och de hade ingen starkare invändning.

NN har känt sig ganska ensam i detta. 2020 april började NN på kth och var ny. De första månaderna pratade han med robin och patrik. Då var gdpr väldigt nytt. De som börjar idag får kanske mer färdiga regler kring detta.

Vems är ansvaret att data hanteras korrekt? Lärosätet eller forskare eller kanske karolinska. NN tror inte att det är karolinska iaf. Frågan bör ställas till en jurist.

NN har uppfattat det som att han är ansvarig genom delegation från prefekt att det är han. Övergripande ansvaret har skolan men delegerat till NN operativt.

8. Hur säkerställs att data hanteras rätt utifrån klassning/"känslighet"?

Lärosätet har inte följt upp det hittills.

Inom avdelningen – NN har en kontinuerlig dialog med de studenter han handleder, doktorander frågar är det ok att jag hanterar data såhär och såhär, vilket NN tycker är positivt med dialogen.

9. Vilka har behörighet att komma åt och se din forskningsdata?

Patientbilder – de som behöver kunna se den. Restriktiva även inom gruppen, läkare på karolinska och avdelningen inom X ca 10 personer – olika personer har tillstånd att se olika saker, tex GE-avtal, finns personligt sekretessavtal företagshemligheter. Finns några personer på avdelningen som inte får se den ge-datan, men får se forskningsdatan som inte är skyddsvärd.

Snävast kategorin patientbilder = de personer som behöver dem.

Delar inte utanför avdelning kth, om inte tillstånd tex läkare kth för det är ju deras bilder.

Det enklaste är om tex karolinska delar och tar ansvar för det och sen sprider det till andra för då tar de ansvar.

10. Tas backuper på din forskningsdata? Görs återläsningstester av backuperna?

NN har inte varit jätteduktig på att fråga om backuper görs. NN gör det på egen dator som han personligen administrerar. Gärna varje vecka. Återläsningstest: det blir lite som det blir, testar ibland om filen kom över som den skulle. Återläsningstest: inga rutiner för det.

Krypterad hårddisk pratar han också om.

11. Lagt till. Om du behöver stöd/hjälp – vet du var du kan vända dig?

Patrik, Robin och Rosa. Lite oklart vem av dem i olika frågor. Rosa har han fått kontakt med nyligen men han kan tänka sig att just infoklassningsfrågor ska ställas just till henne.