UiT
NORGES
ARKTISKE
UNIVERSITET

Avdeling / Institutt / Enhet
Arkivref.:
Dato: 04. mai 2017

Saksnr: xxx

SIKKER HÅNDTERING AV SENSITIVT VIDEOINNHOLD

Til: **ITA/ROS-analyse ansvarlige**
Periode: Vår 2017

Bakgrunn
Høsten 2016 ble det avdekket manglende konsesjon for studenters bruk av video i undervisning ved Helsefak. Enkelte svakheter i rutinebeskrivelser ble også avdekket og fulgt opp.

Dette notatet er en kartlegging både av pågående aktiviteter og fremtidige behov ved helsefagutdanningene som er en del av arbeidet med en konsesjonssøknad til datatilsynet. Her skal vi se på enkelte trinn i håndtering av sensitiv video i forbindelse med undervisning. Omfanget begrenses til det Helsefak har beskrevet som nødvendig i nær fremtid, og løsningsforslagene til det som er realistisk gjennomførbart på kort sikt. Der det er naturlig skisserer vi også andre aktiviteter med lignende arbeidsprosesser eller sikkerhetskrav og hvordan vi på lengre sikt kan lage løsninger som gir bedre støtte til oppgaver av lignende karakter.

Avgrensninger: to typer bruk av video
Scenario 1: det store volumet av innmeldte behov beskriver *opptak av interaksjon mellom en student og en pasient*. Hensikten med opptaket er typisk at studenten skal kunne få tilbakemelding på sin adferd fra en veileder og kanskje en liten gruppe medstudenter fra samme veiledningsgruppe. Opptaket vil normalt slettes etter kort tid og etter et lite antall visninger - ofte bare én - i kontrollerte omgivelser. I noen tilfeller vil det være behov for kopifremstilling og avlevering av kopi til veileder. Kopien skal da også slettes senest samtidig som originalen.

Scenario 2: i mindre omfang beskrives behov for bruk av sensitiv *video som læremiddel der visning er bruker-initiert*, varer over lengre tidsrom og det er svakere kontroll på omgivelsene der tittingen foregår. Dette er en vesensforskjellig prosess som krever andre løsninger og gir annen risiko. Slik aktivitet er ikke nært forestående og diskuteres mer under.

Prosessanalyse og beskrivelse av trinnene

- I det følgende brukes ordet «visning» om situasjonen der studenten som besitter opptaket spiller dette av fra en lokal kopi (m.a.o. **ikke** strømmet over nett) fremfor én (eller få personer) for å få en tilbakemelding.
- Situasjonen der en veileder alene ser på en lokal kopi (typisk som forberedelse før en visning) kalles et «gjennomsyn».
- I tilfeller der en bruker ser på et opptak gjort tilgjengelig via nett kalles en «avspilling».
- Fremstilling og formidling av kopi kalles en «Overlevering».
- Mer generelle tilfelle av transport (innlevering, opplasting) og deling, samt skille mellom sikre og usikre soner kommer ikke til anvendelse her – men se «Utvidelser» under.

Tabell A: scenario 1 – mulige trinn

Aktivitet / oppgave / trinn		Typisk sted eller hensikt	ID
Opptak og lagring			
	Eget utstyr	Legekontor, hos pasient, UIT/UNN-rom	O1
	Fastmontert utstyr	Universitetsklinikk	O2
Overlevering (til gjennomsyn)			
	Fysisk til stede	Samtidig på samme sted	K1
	Fysisk transport av opptak	Kort avstand i tid / rom	K2
	Via nett	Når avstand / tid forhindrer fysisk levering	K3
Visning			
	Direkte fra eget utsyr	Veiledning / veiledningsgruppe	V1
	Direkte fra eget utstyr	Forelesning	V2
	Via nett	1-1 Veiledning over avstand	V3.1/.2
	(Gjennomsyn)	Som V1 men uten publikum	(V1)
Sletting			
	Egen kopi	Etter visning	S1

Tabell B: Scenario 2 – nye trinn

Aktivitet / oppgave / trinn		Kommentar	ID
Opptak og lagring			
	Kamera	Om O1 ikke egnet	O3
	Sikkert lager	Så snart som mulig etter opptak, optimal løsning er å skrive direkte til kryptert lagringsenhet	L1
Redigering / behandling			
	Eget utstyr	Antatt utført av fast ansatt	R1
	Sikker container	Planlagt men ikke innført	R2
Publisering			
	Opplasting til videotjeneste		L2
	Brukerinitiert avspilling	Liten kontroll på omgivelser	V4
Sletting			
	Kamera	Krever sikker sletting	S2
	Publiseringsløsning	Krevende	S3

Tekniske løsninger og rutiner

Sammenlignet med en generell beskrivelse av en videos livssyklus med opptak – redigering – kopiering - distribusjon - publisering - konsum – arkiv – sletting, er trinnene i tabell A ovenfor en liten - og i et teknisk perspektiv - enkel delmengde. I forslag til løsning har vi lagt vekt på:

- Tekniske løsninger med lav bruksvanskelighet
- Prioritere beskyttelse mot *innsyn i personsensitive data,* ikke *tap av data*
- Løsninger som kan implementeres innen rimelig tid og med lave kostnader

For scenario 1 anbefaler vi at studenter benytter selveid bærbart utstyr og laptopens innebygde kamera (evt. et USB-tilkoblet web-kamera dersom kvalitetskrav eller opptakssituasjonen krever det). For lagring brukes forhåndskrypterte minnepinner, fortrinnsvis en variant med integrert kode-tastatur. Dette gir lav brukerterskel og få trinn som reduserer potensialet for feil bruk. Det forutsettes videre at alle anbefalte prosedyrer er beskrevet og at denne dokumentasjonen er kjent og tilgjengeliggjort for studentene det gjelder og til rett tid.

Tabell C: anbefalte løsninger for scenario 1

ID	Beskrivelse
O1	Opptak gjøres med innebygget eller USB-tilknyttet kamera og bærbar datamaskin (IKKE telefon eller annen mobil enhet) Lagring skjer direkte til *kryptert minnepinne* som er beskyttet med passord og/eller pin.
O2	Fastmontert kamera er USB-tilknyttet en stasjonær eller bærbar maskin. Lagring skjer som i O1.
K1	Eier og mottagers krypterte minnepinne tilkobles samme maskin, data overføres ved direkte kopiering.
K2	Eier kobler to krypterte minnepinner til samme maskin, overfører ved direkte kopiering. Kopien overleveres eller avleveres på sted den er tilgengelig for mottager. Mottager får passord / pin til den kryptert minnepinne via annen kanal som lynmelding eller SMS.
K3	Kun unntaksvis nødvendig. Videoen krypteres ved å pakkes i kryptert filarkiv (.zip-fil). Dokumentasjon gjøres tilgjengelig via UITs nettsider for brukerstøtte og vil der anbefale programmet 7Zip og AES-256 kryptering. Overføring skjer via tjenesten *Filesender*. Mottager får passord til .zip-fil i annen kanal.
V1	Eier spiller av direkte fra en kryptert minnepinne. Bilde vises på direkte tilkoblet skjerm / prosjektør.
V2	Som for V1 evt. med en forutgående overlevering. Skiller seg fra veiledningsgruppe-scenarioet ved at avtalt oppbevaringstid kan være lenger. Om nødvendig kan kopi for sikring mot tap fremstilles som i K1/2.
V3.1	Unntaksvis er veileder og student ikke i samme rom ved veiledning; avspilling skjer som i V1, skjermbilde gjøres tilgjengelig for veileder via skjermdeling i UiTs videotelefoniløsning (Skype for Business).
V3.2	Strengt tatt ikke en vising. Veiledning skjer som i 3.1 via video-telefoni, men uten avspilling; Veileder har på forhånd sett video etter å ha mottatt kopi og foretatt «gjennomsyn».
S1	Filer på krypterte minnepinner kan slettes ved vanlig sletting.

Scenario 2 byr på flere utfordringer. Den løsningen vi i dag bruker for forskningsprosjekter med krav til sikkerhet (TSD – tjenester for sensitive data) er ikke uten videre egnet. Om sensitiv video (eller annen personsensitiv informasjon) skal inngå i elektroniske læremiddel i særlig omfang, vil det kreve systemer vi bare på tegnebrettet i dag. Under skisserer vi likevel hvordan enkeltprosjekter som behandler innhold som er sensitivt, men ikke har særlige høyt skjermingsbehov, kan gjennomføres med dagens løsninger ved hjelp av tillemping av metoder fra Scenario 1.

Utfyllende beskrivelser vil være påkrevd om det skal realiseres.

Tabell D: løsningsforslag til scenario 2

ID	Beskrivelse
O3	Ved bruk av håndholdt kamera må det brukes ett som har løst minnekort. Her vil det ligge en ukryptert kopi som sikres fysisk til den er kopiert til lagringsenhet (L1).
L1	For prosjekter der videoer skal etterbehandles anbefaler vi eksterne harddisker med maskinvarekryptering og integrert tastatur. For sikring av data mot tap kan sikkerhetskopi tas til kryptert minnepinne (K1).
R1	For redigering på eget utstyr monteres lagringsenhet (L1) og det arbeides mot denne. Siden potensialet for arbeidskopier på maskinen er til stede må også denne å ha kryptert filsystem (UITs gjeldene regime med Bitlocker på bærbare PC'er vil være akseptabelt)
R2	For delt arbeid vil fjerntilgang til en sikker sone med lagring og nødvendig programvare være nødvendig. I påvente av egnet lokale løsninger anbefaler vi at eventuelle slike aktiviteter benytter TSD
L2	Den ferdige video kan lastes opp fra L1 montert på egen maskin til korrekt mappe i UITs videosystem (pt Mediasite) via web (https).
V4	Styring av tilgang til innhold i videostrømmingstjenesten vår gjøres via krav om pålogging og medlemskap i tilgangsgrupper
S2	Etter at innhold er overført fra minnekort til egnet lagringsenhet (L1) må kortet slettes ved hjelp av programvare for sikker sletting. (Oppskrift for dette vil finnes på UIT's nettsider for brukerstøtte)
S3	Etter avtalt periode må innholdet fjernes fra UIT's publiseringsløsning. Her vil vi ikke kunne garantere sikker sletting, ei heller presis angi når siste kopi er borte fra Backup

Arbeidsprosessene skissert ovenfor skalerer kun i liten grad. Publiseringsregimet er heller ikke særlig egnet for innhold der utilsiktet visning kan få store negative konsekvenser.

For forskningsformål har vi enkeltløsninger der både delt redigering og bruker-initiert (men betydelig mer kontrollert) visning er mulig. En sikker infrastruktur som trygt og effektivt vil kunne benyttes til undervisningsformål er planlagt. Frem til løsningen foreligger, bør bruken av sensitivt innhold i elektroniske læremiddel begrenses til slike tilfeller der innholdet tidligere ville kunne vært distribuert i et større antall fysiske kopier.

Informasjonen som gis til deltagere må gjenspeile denne situasjonen.

Notatet er i hovedsak forfattet av Stig Wennevold og deretter redigert av Jan Ketil Petersen.

På vegne av de involverte i «krypteringsprosjektet» ved ITA
Jan Ketil Petersen
IT-rådgiver, Seksjon for digitale utdanningstjenester
–
jan.k.petersen@uit.no