

To: (10)(2e) <(10)(2e)@rivm.nl>
From: (10)(2e)
Sent: Mon 9/7/2020 3:01:14 PM
Subject: RE: Wil je hier even naar kijken?
Received: Mon 9/7/2020 3:01:15 PM
[veilig stellen e-mail TM.docx](#)
[veilig stellen tekstberichten TM.docx](#)

Hallo (10)(2e)

Hierbij mijn opmerkingen en twee bijlagen m.b.t. het veiligstellen van e-mail en tekstberichten. Deze bijlagen zijn nog niet definitief dus graag (nog) niet delen. In het algemeen is het misschien beter om je formulering iets aan te passen en je toon iets te matigen. Inhoudelijk klopt je verhaal.

Groeten,
 (10)(2e)

From: (10)(2e) <(10)(2e)@rivm.nl>
Sent: maandag 7 september 2020 15:59
To: (10)(2e) <(10)(2e)@rivm.nl>
Subject: Wil je hier even naar kijken?

Hallo allemaal,

Ik stuur deze mail in reactie op de mail van (10)(2e) c.s.

Juridisch toegestaan

(10)(2e) schrijft (terecht) dat dit nog te bepalen is. Maar voor een groot deel liggen de contouren ook vast in wet- en regelgeving en beleid. Voorbeelden hiervan zijn:

- De Archiefwet definieert als criterium voor archiefbescheiden (in het nieuwe Archiefwetsvoorstel "documenten" genoemd) als documenten die "naar hun aard" bij de organisatie die zij heeft dienen te berusten. Documenten die in strijd met wet- en regelgeving bij het RIVM berusten zijn dat per definitie NIET. Documenten die door het RIVM zonder geldige grondslag en/of doelbinding worden verwerkt in de zin van de AVG zijn dus per definitie (zo je wil: juridisch) NIET archiefwaardig en behoren volgens mij geen deel uit te maken van het COVID-19 dossier dat het RIVM uiteindelijk oplevert.
- De Archiefwet maakt GEEN onderscheid in de vorm van documenten. Voor bijvoorbeeld Word-, Excel-, en Powerpointdocumenten, emails, databases, persberichten, websitepagina's, chats zoals What's app en andere social media etcetera geldt dat zij onder de archiefwet vallen;
- De AVG op zijn beurt stelt duidelijke eisen aan het verwerken en dus ook aan het bewaren, opslaan en archiveren van documenten. Daaraan zal voldaan moeten worden, willen documenten überhaupt voor archivering (lees: opname in het uiteindelijk op te leveren COVID19 dossier) in aanmerking komen;
- De AVG stelt ook nadrukkelijk dat documenten gepseudonimiseerd/geanonimiseerd kunnen worden in plaats van in zijn geheel uitgesloten te worden van archivering.
- Het VIR-BI is duidelijk over wat er bij het rubriceren van documenten dient te gebeuren. De behandelaar stelt de rubricering en de duur van het rubriceren voor. De leidinggevende als procesverantwoordelijke stelt de rubricering EN de duur ervan vast. Dit is hiermee een verantwoordelijkheid van het primaire proces.
- Gerubriceerde documenten zijn documenten die onder de Archiefwet vallen. De PROCEDURE van archiveren, onder anderen het overdragen aan het NA (daarbij worden in zo'n geval beperkingen aan de inzage gesteld), de bewaarcondities en condities voor toegang tot/inzage in deze documenten verschilt van die van ongerubriceerde documenten.
- De DG heeft al besloten dat de persoonsgegevens in de Infectie-Radar geanonimiseerd moeten worden vóór de database wordt gearchiveerd. Of dit bij andere databases en toepassingen ook dient te gebeuren is momenteel in bewerking. Veel hangt hierbij af van de grondslag en doelbinding van deze databases. Het kan dus zijn dat voor verschillende databases verschillende archiefregimes gelden.

Toepassing

De toepassing en naleving van wet- en regelgeving is kennelijk bij het RIVM een zaak van een andere orde. Voorbeelden hiervan uit de mail van (10)(2e) zoals ik hem begrepen heb zijn: (opmerking: ik zou deze zin weghalen).

- In RIVMDoc zijn tot dusverre een kleine 400 documenten rondom COVID19 opgenomen. Dit inschattende lijkt me dit slechts een klein percentage van de documenten die het COVID19 dossier op dit moment zou moeten bevatten.
- Daar waar (10)(2e) schrijft dat rubricering voor "het overgrote deel" NIET wordt toegepast is dit volgens mij toch echt een verantwoordelijkheid van in eerste instantie de behandelaar in kwestie (stelt rubricering en de duur ervan voor) en uiteindelijk de proceseigenaar (stelt e.e.a. vast). En deze verantwoordelijkheden dienen volgens mij dan gekend EN nageleefd te worden. Als datgene wat (10)(2e) schrijft inderdaad de werkelijkheid is (en wie ben ik om eraan te twijfelen) zou het hele COVID19 dossier een aaneenschakeling van (potentiële) veiligheidsincidenten zijn. En voor veiligheidsincidenten (kennis hebben van, aangifte doen, optreden) gelden ook weer regels. Dit geldt temeer voor documenten die een hogere rubricering dan DEP V hebben of zouden krijgen want die mogen, de mail van (10)(2e) gelezen hebbende, niet eens op de netwerkinfrastructuur van het RIVM staan (dus ook niet op persoonlijke- en afdelingsschijven, emailboxen etc.);
- Rubriceringen (en merkingen) in RIVMDoc kunnen ook op hogere niveaus dan het documentniveau worden gedefinieerd. Met het plaatsen van een document in die map "erft" het document de rubricering van de map. Punt is, dat met een verstandige mappenindeling volgens mij veel van het manuele rubriceringswerk vermeden/geautomatiseerd kan worden. Het zou daarbij best handig zijn naar mijn mening als het rubriceringsniveau ook op de documenten geplaatst zou worden en als bijvoorbeeld DocGen hiervoor in al zijn sjablonen de mogelijkheid zou geven, dit standaard aan email zou kunnen worden toegewezen etc.
- Databases worden na de COVID19 crisis ter archivering aangeboden. Per database zou volgens mij dan bekeken moeten worden of de database in zijn geheel, of bijvoorbeeld een geanonimiseerde subset onderdeel uitmaakt van het uiteindelijke COVID19 dossier.
- **Inzake emails: Emails kunnen zodanig worden gearchiveerd dat gepseudonimiseerd of geanonimiseerd gebeurt. Gevoelig liggende verzenders en ontvangers kunnen worden geblanked namen en andere persoonsgegevens in de betreffende email ook.** Er wordt alleen wat van de waakzaamheid van de steller (bij interne email en email die naar een adres buiten de organisatie wordt verstuurd) of de ontvanger (externe email die gericht is aan een of meer medewerkers van het RIVM) verlangd;
- **Mailboxen die belangrijk genoeg zijn om in het hotspotdossier opgenomen te worden zullen in het kader van het CARVE project worden geïnventariseerd, bewerkt (geschoond van irrelevante informatie) en gearchiveerd in het COVID19 dossier. (opmerking: zie bijlage voor strategie veiligstellen e-mails sleutelfiguren).**
- De voorgestelde gelaagdheid in toe te kennen rubriceringen uit de mail van (10)(2e) is mij niet duidelijk. Met name: wat wordt bedoeld met "hoe verder van de COVID19 processen af"? Archiveren moet overigens ALTIJD, tenzij er sprake is van documenten die de organisatie verwerkt in strijd met wet- en regelgeving. Anders overtreedt je de Archiefwetgeving weer.
- Consulteren van de OR: dat is volgens mij aan degenen die hierover beslissen. Ook voor wat instemmings- en adviesplichting is aan de OR gelden regels (zoals onder meer verwoord in de Wet op de Ondernemingsraden).

Knelpunten

- De archivering van het COVID19 dossier loopt niet "op schema";
- Hetzelfde geldt voor het manueel rubriceren van stukken (met name van individuele documenten die zwaarder gerubriceerd zouden moeten worden dan de rubricering van de map is waarin zij geplaatst worden in RIVMDoc). Over de documenten die eventueel BUITEN RIVMDoc geplaatst worden doe ik in dit verband geen uitspraken;
- De mogelijkheden met betrekking tot rubriceren, autoriseren, opslaan en ontsluiten van de verschillende ter beschikking staande systemen wordt niet optimaal benut;
- De wettelijke regels, zoals de AVG, beveiligings wet- en regelgeving, openbaarheidswetgeving (zoals de uitzondering op persoonlijke meningen) en de Archiefwet- en regelgeving worden vaak niet in acht genomen.

Advies

- Daar waar de gesignaleerde knelpunten te wijten zijn aan een gebrek aan kennis bij de verwerkers en proceseigenaren binnen de organisatie (ook bij de besturende en ondersteunende processen), is de principiële keuze er één tussen achteraf manueel of geautomatiseerd herstellen (de in (10)(2e) woorden "bewerkelijke en complexe route") of instrueren van de medewerkers van het RIVM. Die laatste optie geldt dan voor de documenten die in het vervolg van de COVID19 crisis aan het dossier worden toegevoegd. Om de route zo min mogelijk bewerkelijk en complex te maken zal er volgens mij dus aandacht aan instructie aan de gebruikers

moeten worden gegeven. FCC/IB zou dit naar mijn mening moeten doen op het gebied van informatieveiligheid, het Centraal Archief in de instructie over de omgang met RIVMDoc.

- Voor documenten met een hogere rubricering dan DEP V geldt dat de procedure voor archivering door de proceseigenaar moet worden afgesproken met het Centraal Archief (CA). Voor fysieke documenten heeft het CA een standaard procedure. Voor digitale documenten is archivering (afhankelijk van het type document (Office bestand, database, chat, website etc) en de drager (schijf, USB stick, optische schijf etc.) maatwerk.

Met vriendelijke groet,

(10)(2e)

(10)(2e)

Stafeenheid Communicatie en Documentaire Informatievoorziening
Postbus 1
3720 BA Bilthoven

Tel: (030- (10)(2e) / 06- (10)(2e)

E-mail: (10)(2e) @rivm.nl

From: (10)(2e) <(10)(2e)@rivm.nl>

Sent: donderdag 3 september 2020 15:52

To: (10)(2e) <(10)(2e)@rivm.nl>; (10)(2e) <(10)(2e)@rivm.nl>

Cc: (10)(2e) <(10)(2e)@rivm.nl>; (10)(2e) <(10)(2e)@rivm.nl>; (10)(2e) <(10)(2e)@rivm.nl>;

(10)(2e) <(10)(2e)@rivm.nl>

Subject: Covid hotspot

Hallo (10)(2e) en (10)(2e)

Dinsdag vroegen jullie mij naar IB perspectief mbt verzamelen van documentatie nav de COVID-19 hotspot. We hebben erover gesproken.

Ik begreep dat jullie wens is om zoveel mogelijk te automatiseren, gezien de hoeveelheid informatie/documenten/berichten.

Ook begreep ik dat jullie de keus willen laten bij de RIVM medewerkers, er zijn al oproepen (ook vanuit de DG) gedaan om gerelateerde documenten te archiveren.

Voorwaardelijk: lijkt mij om te bepalen wat juridisch is toegestaan. Daarvoor heb ik jullie verwezen naar (10)(2e) en ik zag dat jullie contact met haar hebben gelegd (de mail nog niet kunnen lezen).

Het resultaat van de hotspot is duidelijk, alleen de route daarnaartoe moet ook ordentelijk en (wettelijk)geoorloofd zijn, denk aan verwerking van persoonsgegevens dat niet is toegestaan (AVG) mits je oa een grondslag hebt en er doelbinding is.

Ook het consulteren van de OR lijkt me een noodzakelijke stap (ethisch, proportionaliteit etc). Transparantie lijkt mij vereist.

Onze infrastructuur (netwerk, mailservers) faciliteert het vereiste veiligheidsniveau tm departementaal vertrouwelijk. Er is dus mailverkeer/er zijn dus documenten die DEPT V zijn.

Er is heel veel ongestructureerde informatie, er zullen persoonlijke opinies zijn, privé mailberichten die niet als zodanig gelabeld zijn.

Het overgrote deel is niet gerubriceerd, waardoor de mogelijkheden/verplichten mbt deze informatie niet zondermeer bepaald kan worden.

Rubriceren is een manuele weging bij het RIVM, tooling is er niet (het automatisch (met terugwerkende kracht) classificeren lijkt een bewerkelijke en complexe route).

Mbt de keuze mogelijkheden van mensen; wat als persoon A en B mailen over COVID 19 en persoon A kiest voor manueel (want die stemt niet in met data scraping) en B voor automatisch.

Hoe worden dan beide keuzes gerespecteerd?

Gezien de omvang en belasting vd organisatie; indien mogelijk lijkt het zinvol om de 'kern COVID 19' (zoals decision makers) het strengste regime te laten ondergaan mbt archivering.
En zo een gelaagdheid toe te passen, hoe verder van de COVID-19 processen af, hoe minder impact voor de betrokkene om de documenten/informatie te archiveren.

Succes en ik hoop dat dit helpt. Mijn collega's (10)(2e) en (10)(2e) hebben met mij meegedacht.

GR

(10)(2e)

(10)(2e)
(10)(2e) (10)(2e)
Rijksinstituut voor Volksgezondheid en Milieu
Stafeenheid Finance, Compliance en Control (FCC) | Werkplek (10)(2e)
Afdeling Safety & Security

Postbus 1 / postvak (10)(2e) 3720 BA Bilthoven
Antonie van Leeuwenhoeklaan 9 | 3721 MA Bilthoven
T: 030 (10)(2e) | M: 06 (10)(2e)
www.rivm.nl | RIVM, de zorg voor morgen, begint vandaag.

NB bij bezoek aan het RIVM dient u zich te legitimeren (geldige Rijkspas/geldig Identiteitsbewijs).
Indien geen geldig Identiteitsbewijs kan worden getoond, wordt de toegang tot het RIVM geweigerd.
Legitimatiebewijzen van andere organisaties worden niet geaccepteerd.