

# Accione una infracción DLP para probar una directiva HIPAA en el ESA

## Contenido

[Introducción](#)

[Accione una infracción DLP para probar una directiva HIPAA](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo probar la portabilidad y la Data Loss Prevention del acto de la responsabilidad (HIPAA) (DLP) del seguro médico una vez que usted ha habilitado el DLP en su directiva saliente del correo en su dispositivo de seguridad del correo electrónico de Cisco (ESA).

## Accione una infracción DLP para probar una directiva HIPAA

Este artículo proporciona un cierto contenido real, que se ha modificado para proteger a la gente, para probar contra la directiva DLP en su ESA. Esta información se diseña para accionar en el HIPAA y el Information Technology de la salud para la directiva económica y clínica DLP de la salud (ALTA TECNOLOGÍA) y también acciona otras directivas DLP como el número de la Seguridad Social (SSN), CA AB-1298, CA SB-1386, y así sucesivamente. Utilice la información cuando usted envía un correo electrónico de la prueba con su ESA o cuando usted utiliza la herramienta de la **traza**.

**Nota:** Usted debe utilizar un SSN válido o comúnmente empleado mal en la salida donde en **negrita**.

**Nota:** Para la directiva DLP HIPAA y de la ALTA TECNOLOGÍA, asegúrese de que usted haya configurado los números de identificación personalizados según lo recomendado. Números de identificación pacientes (arreglo para requisitos particulares recomendado) O identificador nacional del proveedor E.E.U.U.O diccionarios del número de la Seguridad Social Y de la atención sanitaria E.E.U.U. Usted debe hacer esto configurar para accionar correctamente.

Procedure Notes

Progress Notes

Archie M Johnson Tue Jun 30, 2009 10:31 AM Pended

June 30, 2009

Patient Name: Gina, Lucas DOB: 01/23/1945

Telephone #: (559) 221-2345

SS#: **[[[PLACE SSN HERE]]]**

-----  
Insurance: UHC

How was the patient referred to the office: \*\*\* (:{:20})

Is a family member currently being seen by the requested physician? {YES/NO:63}

If yes, what is the family members name : \*\*\*

Previous PCP / Medical Group? \*\*\*

Physician Requested: Dr. \*\*\*

REASON:

1) Get established, no current problems: {YES/NO:63}

2) Chronic Issues: {YES/NO:63}

3) Specific Problems: {YES/NO:63}

Description of specific problem and/or chronic conditions:

{OPMED SYMPTOMS:11123} the problem started {1-10:5044} {Time Units:10300}.

Any Medications that may need a refill? {YES/NO:63}

Current medications: \*\*\*

-----  
Archie M Johnson

Community Health Program Assistant Chief

Family Practice & Community Medicine

(559) 221-1234

Lucas Gina Wed Jul 8, 2009 10:37 AM Pended

ELECTIVE NEUROLOGICAL SURGERY

HISTORY & PHYSICAL

CHIEF COMPLAINT: No chief complaint on file.

HISTORY OF PRESENT ILLNESS: Mary A Xxtestfbonilla is a \*\*\*

Past Medical History

Diagnosis Date

- Other Deficiency of Cell-Mediated Immunity

Def of cell-med immunity

- Erythema Multiforme

- Allergic Rhinitis, Cause Unspecified

Allergic rhinitis

- Unspecified Osteoporosis 12/8/2005

DEXA scan - 2003

- Esophageal Reflux 12/8/2005

prolosec, protonix didn't work, lost weight

- Primary Hypercoagulable State

MUTATION FACTOR V LEIDEN

- Unspecified Glaucoma 1/06

- OPIOID PAIN MANAGEMENT 1/24/2007

Patient is on opioid contract - see letter 1/24/2007

- Chickenpox with Other Specified Complications 2002

## Verificación

Sus resultados variarán, sobre la base de las acciones del mensaje que usted ha fijado para su directiva DLP. Configure y confirme sus acciones para su dispositivo con un estudio del GUI: **Envíe los arreglos para requisitos particulares de las directivas > de la directiva DLP > las acciones del mensaje.**

En este ejemplo, se fija la **acción predeterminada** para quarantine las infracciones DLP a la cuarentena de la directiva y también para modificar el asunto del mensaje con el "[DLP VIOLATION] prepending".

**Los mail\_logs** deben aparecer similares a esto cuando usted envía el contenido anterior a través como correo electrónico de la prueba:

```
Wed Jul 30 11:07:14 2014 Info: New SMTP ICID 656 interface Management (172.16.6.165)
```

```
address 172.16.6.1 reverse dns host unknown verified no
```

```
Wed Jul 30 11:07:14 2014 Info: ICID 656 RELAY SG RELAY_SG match 172.16.6.1 SBRS
```

```
not enabled
```

```
Wed Jul 30 11:07:14 2014 Info: Start MID 212 ICID 656
```

```
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 From: <my_user@gmail.com>
```

```
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 RID 0 To: <test_person@cisco.com>
```

```

Wed Jul 30 11:07:14 2014 Info: MID 212 Message-ID
'<A85EA7D1-D02B-468D-9819-692D552A7571@gmail.com>'
Wed Jul 30 11:07:14 2014 Info: MID 212 Subject 'My DLP test'
Wed Jul 30 11:07:14 2014 Info: MID 212 ready 2398 bytes from <my_user@gmail.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 matched all recipients for per-recipient
policy DEFAULT in the outbound table
Wed Jul 30 11:07:16 2014 Info: MID 212 interim verdict using engine: CASE spam
negative
Wed Jul 30 11:07:16 2014 Info: MID 212 using engine: CASE spam negative
Wed Jul 30 11:07:16 2014 Info: MID 212 interim AV verdict using Sophos CLEAN
Wed Jul 30 11:07:16 2014 Info: MID 212 antivirus negative
Wed Jul 30 11:07:16 2014 Info: MID 212 Outbreak Filters: verdict negative
Wed Jul 30 11:07:16 2014 Info: MID 212 DLP violation
Wed Jul 30 11:07:16 2014 Info: MID 212 quarantined to "Policy" (DLP violation)
Wed Jul 30 11:08:16 2014 Info: ICID 656 close

```

De la herramienta de la **traza**, usted debe ver los resultados enumerados como esta imagen cuando usted utiliza el contenido anterior en el cuerpo del mensaje:

Data Loss Prevention Processing	
Result:	Matches Policy: HIPAA and HITECH Violation Severity: LOW (Risk Factor: 22)
Actions:	replace-header("Subject", "[DLP VIOLATION] \$subject") quarantine("Policy")

## Troubleshooting

Asegúrese de que usted haya seleccionado la directiva necesaria **DLP directiva del DLP de las directivas > del Administrador de directivas de DLP del correo > Add...** en el GUI.

Revise la directiva DLP según lo agregado y asegúrese de que usted ha especificado su clasificador que correspondía con contenido y de que su patrón de expresión normal es válido. También asegúrese de que usted tenga **Y haga juego con la sección relacionada de las palabras o de las frases** configurada. Los clasificadores son los componentes de la detección del motor DLP. Pueden ser utilizados en la combinación o para identificar individualmente el contenido sensible.

Nota: Los clasificadores predefinidos son uneditable.

Si usted no ve el activador DLP basado en el contenido, también revise las **directivas del correo > las directivas salientes del correo > DLP** y asegúrese de que usted hace la directiva necesaria DLP habilitar.

## Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final](#)
- [ESA FAQ: ¿Cómo puedo hacer el debug de cómo un mensaje es procesado por el ESA?](#)
- [SSA.gov: Números de la Seguridad Sociales empleados mal](#)
- [Probador en línea del regex](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)