Radar Quick Reference Guide
Submitter's Guide

Updated 10/15/2023

Table of Contents

♥CVS Health

Radar Reference Guide
Submitter's Guide

Submitter's Responsibilities Overview

All employees and contractors must report unauthorized access/disclosure to personal and/or confidential information that occurred within a CVS Health-related business (PBM, Retail, etc.) or department to the CVS Health Privacy Office. Information must be accurate and comprehensive.

Login Instructions

When you try to login to Radar, be sure to use:

      1) **Google Chrome is the preferred browser.** Although Firefox can be used, there may be some limitations.

      2) Access Radar via Heartbeat > Legal > Privacy Office > Report a Privacy Incident, or by using the link below:
https://heartbeat.cvshealth.com/sites/our-company/our-organization/legal/privacy-office/report-a-privacy-incident

      3) If prompted with the login window (shown below), enter your Network or Employee ID and password. Do not preface your network login ID with a Domain Name.

          Example:

          1. u00bmgb – OK!

          2. Caremarkrx\u00bmgb – Not OK

      4) The password is the same as your windows password to log onto your computer. (If logging in with employee ID, please use your site minder password, which is the same as Learnet.)

♥CVS Health
Enterprise Login Form

Username

Password

LOGIN

Users working in other networks (Coram and Vendor Sites)

Coram and Vendor Sites associates can access Radar only through Citrix, and should use their CVS provided NETWORK ID to log into Citrix. Once Citrix access is established, launch Chrome and follow the instructions above to access Radar.

Click here for additional help with Citrix logon instructions.

Radar HIPAA Disclosure Forms - After you login, you will be taken to the Radar Disclosure Form portal (see below)
Based on your line of business, select the appropriate HIPAA Disclosure form:
- Select "CVS Health HIPAA Disclosure form" for PBM, Accordant, Coram, CVS Specialty, Med-D
- Select "Aetna HIPAA Disclosure form" for Aetna and HCB affiliates
- Select the "Retail HIPAA Disclosure form" for Retail Pharmacy Omnicare, and MinuteClinic

Privacy incident forms

An incident webform is used to alert the Privacy Office of any event in which personal information has been disclosed to an unauthorized party or used in an unauthorized manner. Please select the appropriate HIPAA disclosure form from the list below immediately after you become aware of a potential unauthorized use or disclosure of personal information.

CVS Health HIPAA Disclosure Form ⊡
Use this form for PBM, Accordant, Coram, CVS Specialty, Med-D disclosures, Novologix, CarelonRx, and Shared Services

Aetna HIPAA Disclosure Form ⊡
Use this form for Aetna and HCB affiliates

Retail & Provider HIPAA Disclosure Form (Retail Pharmacy, Omnicare, Optical, MinuteClinic, Kidney Care employees only) ⊡
Use this form for disclosures that occurred at Retail Pharmacy, Omnicare, Optical, MinuteClinic, and Kidney Care locations. NOT FOR PATIENT SAFETY RELATED INCIDENTS - PLEASE USE THE PATIENT SAFETY/EPSO TOOL.

All fields on the new record are needed in order to process your submission, however, fields with a red asterisk * are required in order to submit. Incomplete forms will be returned to you, and you will be sanctioned if you continue to submit incomplete records.

Creating a New Record

   A. Reporter Section
If not already populated, you will need to enter your information as the Reporter. Do not enter a personal phone number or email address.

Reporter		⌃
Your first name *	**Your last name** *	**Your ID**
Your First Name	Your Last Name	
Your phone #	**Your email**	
	Your.email.address@CVSHealth.com ✕	

   B. Basics Section
1. *Dates*: Provide these dates by selecting the calendar icon. (**Note**: See screen shot below)
   - *Occurred Date:* The date PHI was disclosed, or when a communication or prescription was sent. *If unknown, list the date the incident is being reported.*
   - *First Informed Date*: The date the incident was first reported to you.
   - *Discovered Date:* The date you discovered the incident did involve personal or protected health information.

Occurred

[_____] 📅

First informed   **Discovered**

[_____] 📅   [_____] 📅

2. *Occurrence Location* (PBM & Aetna) –This is related to where the incident originated.

C. Individuals impacted: This field relates to the number of affected individuals involved in the incident. (**Note**: Use Exact number box when possible)

Individuals impacted		
Exact number	**Estimated range**	
	< 100 100 - 499 500 - 1000 > 1000 Unknown	

D. Description: When entering information in the Description section be as descriptive as possible.

Please provide a detailed description of the events that resulted in the incident, including:
- Person impacted
- What happened and why
- How the incident occurred
- Individual details

Description

Description *

E. Order Information (PBM): For order/delivery issue-related incidents

Order Information

For order/delivery issue-related incidents, please include the order number below:

Enter Order #
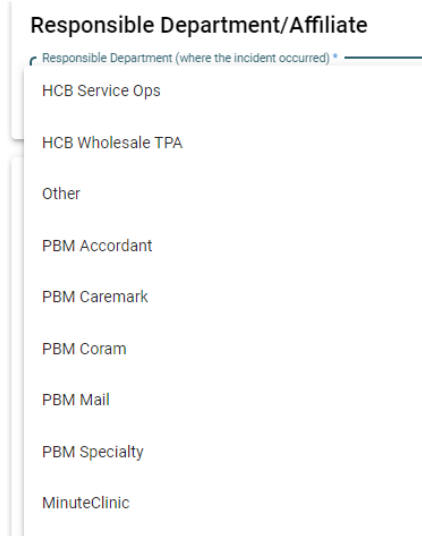
F. Incident End Date: The date PHI was disclosure was completed. *If unknown, list the date the incident is being reported*

Incident End Date

Incident End Date *

G. Responsible Department:

Select where in the organization the incident occurred or was reported, which may be a department, facility, campus, and so on. If the department is not listed, please select "Other" and type in the department name in the space provided
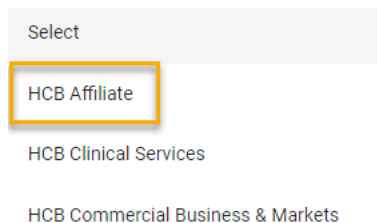
Select "HCB Affiliate" if the incident occurred or was reported by any of our affiliates such Active Health, Student Health, Senior Supplement, etc. Once you indicate an affiliate is responsible, you will be able to select the specific affiliate involved.
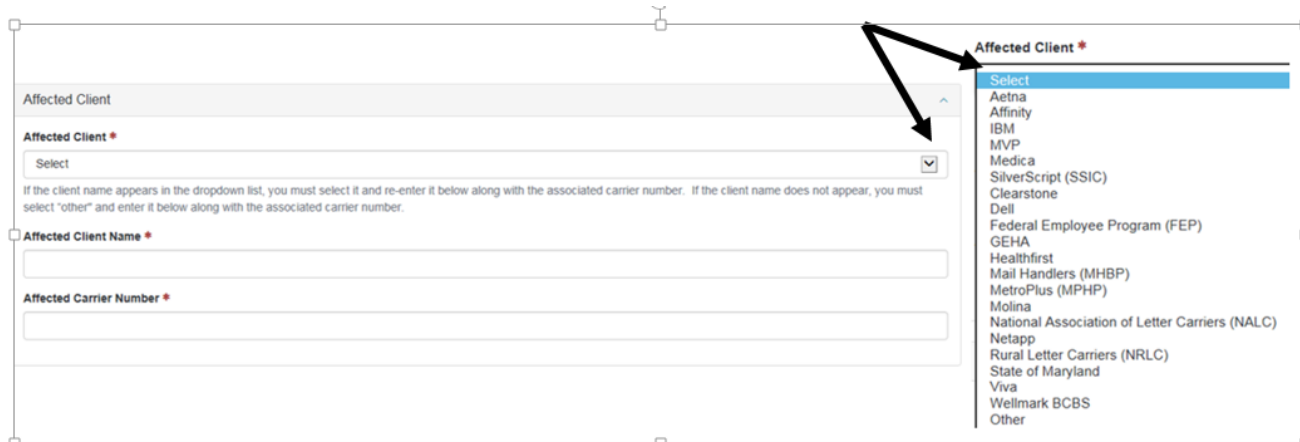
H. Affected Members & Individuals (PBM & Retail): Complete the required information for the affected member(s) or individual(s).

- If the incident involves **additional members listed on the same plan as the initial member (PBM),** you may add **4** additional members in the fields provided and include the member name, member identification number, date of birth, full mailing address and gender on the same line. (**Note:** Incomplete data will be returned)
- If the incident involves **additional individuals (Retail),** you may add **4** additional members in the fields provided and include the name, date of birth, full mailing address and gender on the same line if known. (**Note:** Incomplete data will be returned)
- You may also add additional members or individuals by uploading a spreadsheet after completing the entire Radar Disclosure form. (**Note:** Incomplete data will be returned to you).
  - o For PBM and Aetna, the spreadsheet must contain member name, member identification number, date of birth, full mailing address and gender
  - o For Retail, the spreadsheet must contain the individual's first and last name, address, and Rx Number
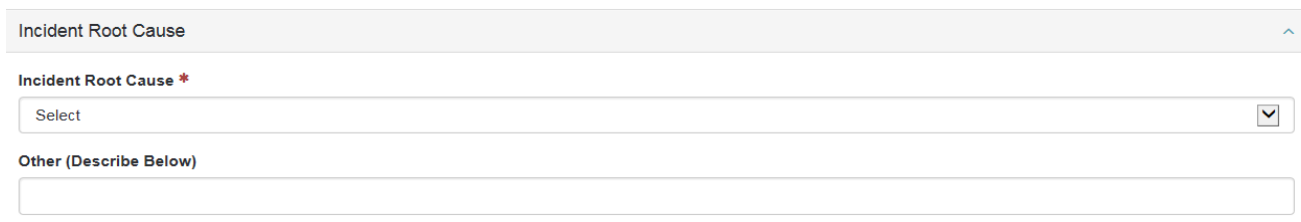
See page 10 on Submitting a disclosure and Page 11 on Uploading Attachments

I. Affected Client (PBM & Retail): This is the Client name associated with the Member whose information was disclosed.

- Click on the dropdown menu to select the A**ffected Client**, **and then enter the Client Name and Carrier Number in the required fields below.**
- If the client name associated with the affected member is not listed, select "Other" from the available list and enter the Client Name and Carrier Number in the required fields.

J. Incident Root Cause: This field allows you to select where the root of the issue occurred.

- Click on the dropdown menu and select an option from the available list.
- *Only* select "Other" if an option from the available list does not match the Root Cause for your submitted incident. When selecting "Other" you are required to provide detailed information in the Describe Below field.

K. Point of Origin (PBM): This field is for indicating where within the business the issue occurred.

L. Retail Location Information (Retail): Enter the store or call center information where the incident occurred

- Store #: Begin to type in your store's ID number or name, and select the correct location
    - For Retail and MinuteClinic call centers, type in **Retail Pharmacy Care Call Center** or **MinuteClinic Support Center**
    - If the store number is not known, or is not listed, type in **Unknown**

- Location Address and City State Zip: Begin to type in your store's Address information and select the appropriate information

M. Recipient of Information
- If the name of the Receiver is known, provide the **Name of Receiving Person or Entity**, and then select what kind of entity received the information e.g. health care provider, physician office, clinic, hospital, retail business etc. from the drop down menu.
- Enter the Address of Receiver if known.
- If the name of the Receiver is not known, type in "unknown".

N. Verbal Assurance (PBM & Retail): *Representatives should be asking callers and those reporting* potential HIPAA disclosures the question as to whether the recipient agrees to not use or disclosure the information and that it has not been retained for any purpose. Select Yes or No to identify if this action has been taken.

Verbal Assurance

Verbal consent was obtained from the person or entity; they agree not to use, not to disclose and not to retain the information for any purpose. *

○ Yes
○ No

O. Responsible Person Information: This section is where you can give details on who is responsible for disclosing the information.
- If known, enter the responsible person's **Name, Title, and Address.**
- Indicate whether the person responsible is an employee
    - If this is an employee issue, select if the employee has been sanctioned.
    - If the employee has been sanctioned, please select a value from the **Type of Sanction** drop down menu. If the sanction is not listed, please provide details in the Other field.

Responsible Person Information

Responsible Name and Title

Responsible Address

Enter Street, State, Zip of responsible person if known

Is this an Employee issue?
○ Yes
○ No

Was the employee sanctioned?
○ Yes
○ No

Type of sanction

Select

Other

P. Action Performed by Recipient: This section refers to what actions have already been taken.

- Click on the dropdown menu to select what the receiver did with the disclosed information.
- If you select "other", you must enter a response to the action performed by the receiver.
- If this incident has also been reported to Information Security, click "Yes", and indicate the IR reference number received.

Action Performed by Receiver

Action Performed by Recipient of Information: *

Has this been reported to Information Security?

☑ Yes

Security Incident ID (IR #)

Q. Category and Sub-Category – Category means the format of the PII/PHI at the time of disclosure. For example, did the impermissible disclosure happen over the phone? If so, select "Verbal or visual".

- After selecting the Category, an associated subcategory drop-down may appear. From the available list, click once on the subcategory item that best describes the incident. (**Note:** Only one selection is allowed.)

R. Data Elements: Click Select All or the individual checkboxes of all the data elements that were disclosed

S. Submission to Privacy Office Section

- After completing all the required fields on the Radar form, and if you do not need to add attachments then click Submit at the bottom of the form.

  o After clicking Submit If your form was completed with no errors, you will receive a successful transmission page.

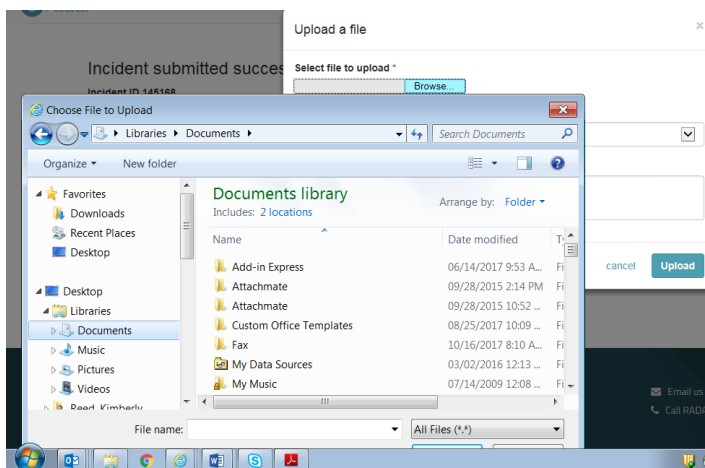 o If you have multiple forms to submit, click ➕ Submit another incident to take you to a new blank form.
  o If you do not have another disclosure to submit, you can exit the form.

T. Uploading/Adding Documentation

- After completing all the required fields on the Radar form, if you need to add attachments, check the "Add attachments" box ☐ Add attachments Submit and then click Submit at the bottom of the form.

  o After clicking Submit If your form was completed with no errors, you will receive a successful transmission page with the upload the attachment (Picture A) box.
  o Click on "Upload attachment" the "Upload a file "screen will appear, (Picture B).
  o Click on Browse (Picture B) to locate the file or document you want to upload (Picture C).
  o Double click the file or document you want to share, the name will appear as the selected file (Picture D).
  o Select the Category (Picture E) to name the item. If selecting "other", provide details in the Description box. (Picture F). Then click Upload.
  o If your upload was done correctly you will receive a successful upload response along with a successful incident submission response (Picture G), and you can submit another incident by clicking "+ Submit another incident" or simply exit the form.
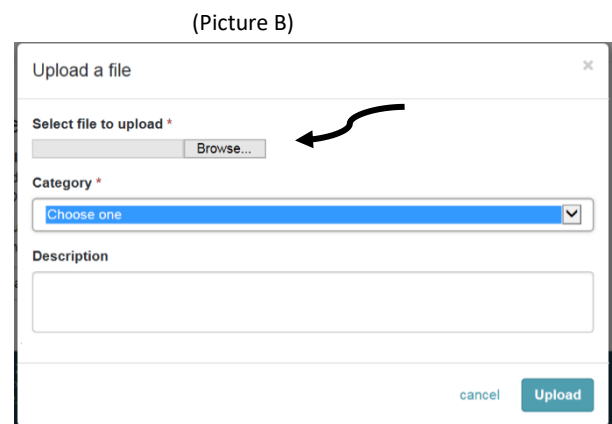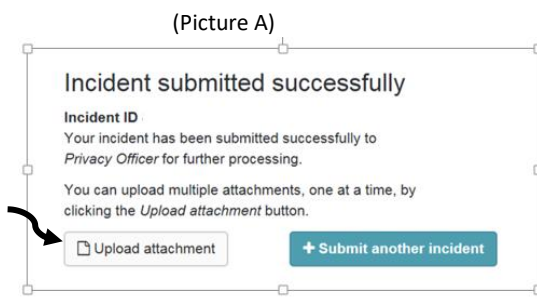
(Picture A)

(Picture B)

(Picture C)

(Picture D)

(Picture E)   (Picture F)

(Picture G)

Tips & Timesavers

- Fields denoted by a red asterisk ***** are required upon submission, and some fields are conditionally (Data Driven Event) required based on the field selection/entry.

- What is a Data Driven Event (DDE)? When selecting an option from a dropdown or ellipsis, your selection might drive a new, previously unseen, required field or section to appear.
    - **For example**; In the Category Section, when you select an action, a new section, Sub-Category, will appear.

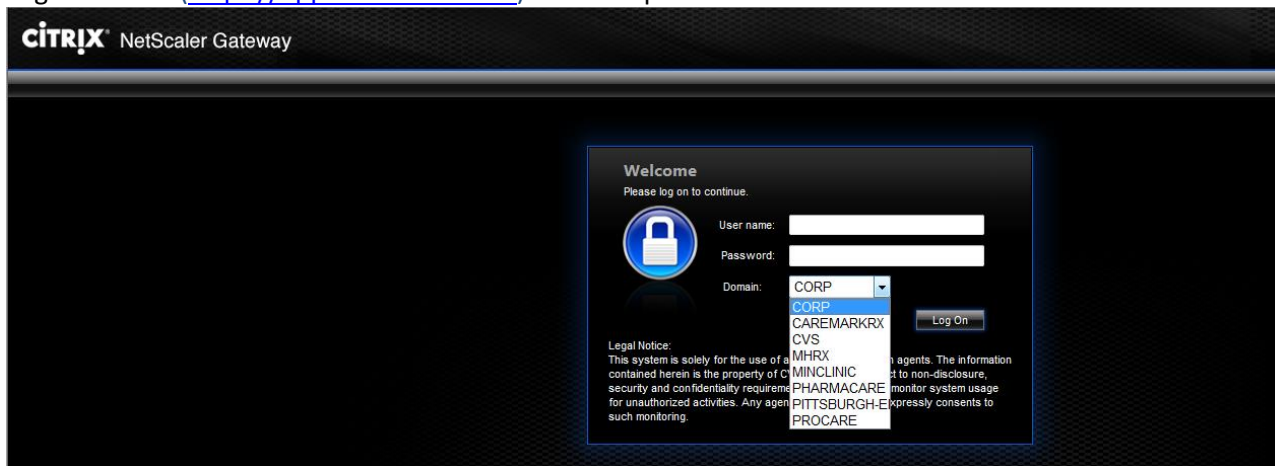- The Radar HIPAA Disclosure forms will automatically log out the user after 2 minutes of inactivity.

Contact Information

If the disclosure issue needs immediate escalation/attention or if the individual specifically requests to speak with the Privacy Office, email:

- For PBM, Accordant, CVS Specialty, and Med-D: PrivacyCaremark@cvshealth.com
- For CVS Retail Pharmacy & Omnicare: PrivacyPharmacy@cvshealth.com
- For Aetna & affiliates: PrivacyAetna@aetna.com
- For Provider (MinuteClinic, Coram, Kidney Care, etc.): PrivacyProvider@cvshealth.com

[Citrix Logon instructions:](#)

1. Login to **Citrix** (https://apps.cvshealth.com) with CVS provided Network ID

2. On the Citrix home page launch Chrome

3. Visit our Privacy Heartbeat page: https://heartbeat.cvshealth.com/sites/our-company/our-organization/legal/privacy-office/report-a-privacy-incident