



Reporting Requirements for Breaches of Confidential Information

Topics

- What is a breach?
- Reporting Breaches
- Information to Include in the Breach Report
- Additional Information That Will Be Required
- Example # 1
- Answer to Example # 1
- Example # 2
- Answer to Example # 2
- Example # 3
- Answer to Example # 3
- Resources

What is Protected Health Information (PHI)?

Care providers are responsible for protecting the following PHI:

- **Health information:** Information, whether verbal or recorded in any form, that you create or receive as a health care provider that relates to the past, present, or future physical or mental health or condition of your patient or any individual.
- **Individually identifiable health information:** Information that is health care-related including demographic information collected from an individual that identifies that person or can be used to identify the person.
- **Protected health information:** Individually identifiable health information that is maintained or transmitted by electronic media or any other form or medium, such as a patient file.

What is a breach?

You and your staff are authorized to use patient information as you serve your patient.

A breach is when someone not unauthorized to use PHI comes into contact with the information by:

- Receiving it
- Accessing it
- Using it
- Disclosing it



Reporting a Breach

You are required to report any breach of your patient's protected health information to:

- Texas Health and Human Services: privacy@HHSCC.state.tx.us

AND

- UnitedHealthcare Community Plan: txcomplianceteam@uhc.com

AND

Our Compliance Officer: deborah_l_deska@uhc.com

Reporting a Breach

When should a breach be reported?

- Within **24 hours** of when you become aware of it

|

If a breach is not reported by this deadline, you may be subject to fines from the U.S. Department of Health and Human Services, Office of Civil Rights.

Information to Include in the Initial Breach Report

Include in your report all available information about the breach, including:

- A description of the breached information
- The way in which the information was breached
- What action(s) you took to protect the information once you became aware of the breach
- Your practice name
- Address
- Phone number
- E-mail address for a single contact person

Important Note: Please include in your report the name of a contact person that can be available both during and after business hours throughout the investigation period.

Additional Information That Will Be Required

Within **48 hours** of reporting the breach, you may be asked to supply additional information, such as:

- Beginning and end dates of the breach
- The date you found out about the breach
- The number of records breached
- A thorough description of the breach, including:
 - Type of breach (hacking, improper disposal of mail, etc.)
 - Location (network server, medical record, etc.)
 - Type of information (clinical, demographic or financial, etc.)
 - Security steps taken to prevent future breaches

Example #1

Dr. Jones keeps patient medical records electronically.

These records are Protected Health Information about patients, including their Medicaid ID, phone numbers, addresses and Social Security numbers.

Despite several protective measures, Dr. Jones learns that someone has hacked into his practice's computer system and gained access to all patient medical records.


Q: How long does Dr. Jones have to report this breach its discovered?

- A. 24 hours
- B. 48 hours
- C. 1 hour
- D. 30 days

Answer to Example #1

Question:

How long does Dr. Jones have to report this breach once he discovers it?

- A. 24 hours 
- B. 48 hours 
- C. 1 hour 
- D. 30 days 

Answer:

Dr. Jones has 24 hours to submit his reports

Example #2

Nurse Betty has a USB flash drive that has on it patient email addresses. Working from home one evening, she uses her husband's computer and doesn't realize that she transferred the entire database to his computer.

Her husband discovers the database two weeks later, but forgets to tell her for another week. She forgets to inform her boss, a primary care physician, until another week later.

Q: What is the starting point for this breach to consider when deciding on the deadline for reporting? When:

- A. The database is transferred to the husband's computer
- B. Her husband discovers the database on his computer
- C. Her husband tells her about the database
- D. She tells the doctor about the database

Answer to Example #2

Question:

What is the starting point for this breach to consider when deciding on the deadline for reporting?

- A. The database is transferred to the husband's computer ❌
- B. B. Her husband discovers the database on his computer ❌
- C. Her husband tells her about the database** ←
- D. She tells the doctor about the database ❌

Answer:

As an employee of the care provider, the starting point for this breach is when Nurse Betty's husband tells her about the database breach.

Example #3

Sue works part-time for a home health agency doing clerical work. In her job she faxes medical records to primary care physicians (PCP). She faxed a set of records Monday afternoon.

When Sue returns to work Wednesday, she learns the records were never received, so she faxes them again. On Friday, she receives a phone call from the PCP telling her that the records still have not been received. Sue then realizes she had faxed the medical record to the wrong fax number.

Question: This does not need to be reported as a breach if the home health agency can confirm that the fax number Sue used was not a valid fax number ,and so, the records did not actually go through to anyone on the receiving end.

A. True

B. False

Answer to Example #3

Question:

This does not need to be reported as a breach if the home health agency can confirm that the fax number Sue used was not a valid fax number ,and so, the records did not actually go through to anyone on the receiving end.

- A. True
- B. False

Answer:

True. This is not considered a breach if the care provider can show that there is a low probability that protected information was actually disclosed.

Resources

Need More Help?



Online:

- For our step-by-step resource guide, go to UHCCommunityPlan.com > For Health Care Professionals > Texas > [Reference Guides](#) > Confidentiality Breach Reference Guide.
- For professional online training, including continuing education, go to HHS.Gov > HIPAA > For Professionals > [Training Materials](#).
- Need help in reporting? call customer service toll-free at [888-887-9003](tel:888-887-9003), 7 a.m. to 7 p.m. Central Time, Monday through Friday.



Thank You.
