Richland County Health and Human Services
Reporting a Breach Event

A breach event is an event where client information is disclosed to an unauthorized person or where client information is at risk of being disclosed. Once you have discovered that a breach event has occurred, you need to follow these steps:

1. Immediately take whatever corrective actions you can do to prevent the breach or to prevent the expansion of the breach. For example, if an e-mail was sent containing the wrong client information, attempt to recall the e-mail before it is read. If a file was accidently left at an unsecured place, attempt to immediately and physically retrieve the file. Once retrieved, examine the file to determine if there is evidence that unauthorized persons likely did or did not see the information.

2. Inform the Richland County Economic Support Manager of what happened using the *"HIPAA Security Incident Report Form."* See attached.

3. The Richland County Economic Support Manager will follow the local agency process found in the HIPAA Policy Manual as directed by Policy # HIPAA 3.10 *"Responding to Improper Disclosures Policy."* This process includes, but is not limited to, evaluating the event and determining the next appropriate steps to take.

4. Stay involved. You and the Richland County Economic Support Manager may need to notify clients or take other steps as directed.

HIPAA Security Incident Report Form

1. Describe the security incident. Please indicate what was observed, where and when it occurred, and who was involved.

2. Describe how the incident was discovered – that is, result of observation, review of audit trails, external complaint, and so forth.

3. Indicate the status of the security incident. Is the incident over? Is it currently ongoing? Has it been recurring?

4. Describe how you think the security incident occurred or how unauthorized access or disclosure happened – that is, hacker, virus, employee misconduct, and so forth.

5. Is the system still at risk of attack?

6. Classify the severity of the incident – high, medium, or low – and indicate whether the response time should be immediate, prompt, or as soon as possible.

7. Describe your assessment of possible systems affected, the clinical, business, and/or administrative functionalities affected, and whether any data, including protected health information ("PHI"), financial information, and/or information that could lead to identity theft, may have been compromised.

8. Please estimate the following or state that not enough information is available for such an estimate:

    a. System downtime:
    b. Damage to the system:
    c. Nature and extent of data lost:
    d. Nature and extent of data improperly disclosed:
    e. Harm, such as financial loss, cost of repairs, possible lawsuits, and so forth:

9. Were the systems of other organizations affected? If so, were they contacted?

10. Indicate the persons that have been notified and the measures taken to address the problem.

11. Indicate your name, title/position, phone number, and email address below in case we need to contact you for further information:

    a. Name:
    b. Title/position:
    c. Work phone number:
    d. Work email address:
    e. Home phone number:
    f. Home email address:

12. Date and time of this report: