

Reports

FIGURE 19.B-1 ANNUAL RISK ASSESSMENT LETTER OF ASSURANCE (SAMPLE)

TRICARE Management Activity (TMA)/Contract Management
16401 E Centretch Parkway
Aurora, CO 80011
ATTN: Administrative Contracting Officer (ACO)

Dear _____:

An annual risk analysis of all systems, policies, procedures and practices of (name of contractor) in effect during the year ended (date) was performed in accordance with requirements outlines in the TRICARE Operations Manual (TOM), [Chapter 19, Section 3](#), and the HHS HIPAA Privacy Rule.

The objectives of the risk analysis were to:

1. Consider both organizational and technical assessments that address all areas of privacy and security.
2. Assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of all PHI (electronic, paper, and oral) created, received, stored or transmitted by the contractor.
3. Take into account all relevant losses that would be expected if privacy and security measures were not in place, including losses caused by unauthorized uses and disclosures, as well as losses of data integrity or accuracy.
4. Determine residual risk.
5. Identify and document an action plan from prioritized findings to mitigate risk to an acceptable level.

The results of the risk assessment, assurances given by appropriate (name of contractor) officials, and other information provided, indicate that the procedures and policies of (name of contractor) in effect during the year ended (**Date**), comply with the requirements in the TOM, [Chapter 19, Section 3](#). The following action plans describe the risk identified during the annual assessment and the plan to correct deficiencies and achieve compliance. Please indicate "NONE" if the annual risk analysis did not identify weaknesses.

Attachment A to this statement contains (1) the (**Name Of Contractor**) plans and schedules for correcting such weaknesses, and (2) the status of actions taken to correct weaknesses identified in prior years' reports.

Sincerely,
Name, Title and Office

FIGURE 19.B-1 ANNUAL RISK ASSESSMENT LETTER OF ASSURANCE (SAMPLE) (CONTINUED)

cc: Regional Director (RD)
TMA Procuring Contracting Officer (PCO)
HA/TMA Privacy Officer
HA/TMA Contracting Officer's Representative (COR)

Enclosure(s) (if any)

Note to Contractor

- (1) If there are no material weaknesses, this sentence should be deleted, and there would be no list or Attachment A containing plans and schedules for correcting such weaknesses.
- (2) If there were no actions taken during the past year to correct weaknesses, or no identified weaknesses for which corrective actions remain to be taken, this phrase would be deleted.

FIGURE 19.B-2 ANNUAL PRIVACY AND SECURITY PROGRAM EVALUATION LETTER OF ASSURANCE (SAMPLE)

TRICARE Management Activity (TMA)/Contract Management
16401 E Centretech Parkway
Aurora, CO 80011
ATTN: Administrative Contracting Officer (ACO)

Dear _____:

An annual privacy and security program evaluation of (name of contractor) in effect during the year ended (date) was performed in accordance with requirements outlined in the TRICARE Operations Manual (TOM), [Chapter 19, Section 3](#), the HIPAA Privacy Rule and the HIPAA Security Rule.

The objectives of the privacy and security program evaluation were to provide reasonable assurance that (name of contractor) is in compliance with:

1. Current practices of the HIPAA Privacy Rule, HIPAA Security Rule, DoD 6025.18-R, HA Policy 06-010 "Health Insurance Portability and Accountability Act Security Compliance," and TMA Privacy and Security requirements.
2. Policies, procedures, processes and practices relating to the confidentiality, integrity and availability of PHI to ensure compliance with the requirements set forth in the TOM, [Chapter 19, Section 3](#).
3. Identify gaps between current policies and procedure relative to HIPAA Privacy and Security requirements.
4. Determine areas of non-compliance and risk.
5. Identify and document an action plan to correct deficiencies.

The results of the privacy and security program evaluation, assurances given by appropriate (name of contractor) officials, and other information provided, indicate that the procedures and policies of (name of contractor) in effect during the year ended (Date), comply with the requirements in the TOM, [Chapter 19, Section 3](#). The following action plans describe the findings identified during the annual evaluation and the plan to correct deficiencies and achieve compliance. [Please indicate "NONE" if the annual evaluation did not identify areas of non-compliance or weaknesses.]

Attachment A to this statement contains (1) the (name of contractor) plans and schedules for correcting such areas of non-compliance and weaknesses, and (2) the status of actions taken to correct areas of non-compliance and weaknesses identified in prior years' reports.

Sincerely,

Name, Title and Office

cc: Regional Director (RD)
TMA Procuring Contracting Officer (PCO)
HA/TMA Privacy Officer
HA/TMA Security Officer
TMA Contracting Officer's Representative (COR)

Enclosure(s) (if any)

FIGURE 19.B-2 ANNUAL PRIVACY AND SECURITY PROGRAM EVALUATION LETTER OF ASSURANCE (SAMPLE) (CONTINUED)

Note to Contractor

(1) If there are no material weaknesses, this sentence should be deleted, and there would be no list or Attachment A containing plans and schedules for correcting such weaknesses.

(2) If there were no actions taken during the past year to correct weaknesses, or no identified weaknesses for which corrective actions remain to be taken, this phrase would be deleted.

FIGURE 19.B-3 PRELIMINARY INCIDENT REPORT FORMAT (SAMPLE)

PRELIMINARY INCIDENT REPORT

Today's Date:

Reporting Organization Information

Reporting Organization's Name:

Location:

Point of Contact:

Title/Position:

Phone/Contact Information:

E-mail Address:

Organization/Location Where Incident Occurred:

Date(s) incident first identified:

Date(s) incident occurred:

Estimated number of affected beneficiaries:

Nature of the incident:

(Include a description of the incident, how incident was discovered, operational areas affected or involved, cause of incident, and resulting outcome of incident.)

Identify data elements involving Protected Health Information (PHI) or Personally Identifiable Information (PII) in this incident?

Do not use specific identifiers (i.e. SSN, Name, DOB) in this report.

Perceived impact on beneficiaries:

Steps taken to date to respond to incident:

Steps taken to mitigate the impact of the incident:

(If PHI or PII was involved you will also need to complete a Risk Mitigation Reporting Form for TMA.)

Mitigation strategies initiated:

(Please note: HIPAA requires mitigation documents be retained for six years.)

Please attach any information not detailed above:

(If data Status Report is necessary the TMA Privacy Office will provide guidance on the incident response documentation and report frequency requirements.)

- END -

