{Comment: Paragraph 1, above, is optional}

(2) **Restriction on Use and Disclosure of Protected Health Information.** Except as permitted or required by this Contract or as required by law, BUSINESS ASSOCIATE shall not use, de-identify, or further disclose any protected health information disclosed or otherwise made available to it by PROVIDER. *{45 CFR §164.504(e)(2)(i) and (e)(2)(ii)(A)}*

{Comment: Paragraph 2, above, is a required provision.}

(3) **Authorized Uses and Disclosures.** Except as otherwise limited in this Contract, BUSINESS ASSOCIATE is hereby authorized to use and disclose protected health information for the following purposes:

(a) **Generally.** BUSINESS ASSOCIATE may use or disclose protected health information on behalf of, or to provide services to, PROVIDER for the following purposes, if such use or disclosure of protected health information would not violate the HIPAA privacy regulations if done by PROVIDER or the minimum necessary policies and procedures of PROVIDER: _____
_____
_____
_____
{45 CFR §164.504(e)(2)}

{Comment: Insert above the general purposes for which Business Associate may use or disclose protected health information. These should fall within the functions, activities and services performed or provided by the Business Associate for Provider. This is a required provision.}

(b) **Management and Administration.** BUSINESS ASSOCIATE may use and disclose protected health information for the proper management and administration of BUSINESS ASSOCIATE or to carry out the legal responsibilities of BUSINESS ASSOCIATE, provided:

(1) The disclosure is required by law; or,

(2) BUSINESS ASSOCIATE obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person and the person will immediately notify the BUSINESS ASSOCIATE of any instances of which it is aware in which the confidentiality of the information has been breached. *{45 CFR §164.504(e)(2)(i)(A) and 45 CFR §164.504(e)(4)}*

{Comment: Subparagraph (b), above, is an optional provision, meaning you do not have to allow the business associate to use electronic protected health information or protected health information for its management and administration.}

(c) Date Aggregation Services. BUSINESS ASSOCIATE may use and disclose protected health information to provide data aggregation services relating to the health care operations of PROVIDER. *{45 CFR §164.504(e)(2)(i)(B)}*

{Comment: Subparagraph (c), above, is an optional provision.)}

(d) Violations of Law. BUSINESS ASSOCIATE may use protected health information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

{Comment: Subparagraph (d), above, is not a required provision.}

(4) BUSINESS ASSOCIATE'S Obligations.

(a) **Representation and Acknowledgment.** BUSINESS ASSOCIATE represents that it has complied and will comply with the requirements of the HIPAA Rules applicable to it and acknowledges that it is aware that it is subject to the tiered civil and criminal penalties of section 1176 and 1177 of the Social Security Act.

[*Comment: Subparagraph (a), above, is optional. The reason to include it is simply to be sure the business associate meets its obligations under HIPAA and is aware of the penalties if it does not.*

The tiered penalties referred to are:

Tier 1. The first tier is for violations the person did not know about and by exercising reasonable diligence would not have known about. It is strict liability, meaning the penalties come into play simply because the disclosure happened. The minimum penalty at this Tier is $100 per violation with an annual maximum of $25,000 for repeat violations. The maximum penalty is $50,000 per violation, with an annual maximum of $1,500,000. However, at this Tier, the Secretary of HHS may still pursue corrective action working with the covered entity to achieve compliance in lieu of imposing penalties.

Tier 2. The second Tier is for violations due to reasonable cause and not due to willful neglect. Violations at this Tier are subject to a minimum penalty of at least $1,000 per violation, with an annual maximum

of $100,000 for repeat violations. The minimum penalty is $50,000 per violation, with an annual maximum of $1,500,000.

Tier 3. *The third Tier is for violations due to willful neglect. Here, the penalty depends on whether or not the violation is corrected.*

If the violation is corrected, the minimum penalty is $10,000 per violation, with an annual maximum of $250,000 for repeat violations. The maximum penalty is $50,000 per violation, with an annual maximum of $1,500,000.

If the violation is not corrected, the minimum and maximum penalty are the same : $50,000 per violation, with an annual maximum of $1,500,000.

(b) **Safeguards.** BUSINESS ASSOCIATE shall use appropriate safeguards, and comply, where applicable, with the HIPAA security regulations with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as permitted or required by this Contract or as required by law. *{45 CFR §164.504(e)(2)(ii)(B)}*

{Comment: Subparagraph (b), above is a required provision.}

(c) **Security of Electronic Protected Health Information.** BUSINESS ASSOCIATE shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of PROVIDER. *{45 CFR §164.314(a)(2)(i)(A)}*

{Comment: Subparagraph (c),above, is a required provision.}

(d) **Reporting.** BUSINESS ASSOCIATE shall report to PROVIDER any use or disclosure of protected health information not permitted by this Contract of which it becomes aware, including breaches of unsecured protected health information as required by the HIPAA Breach Notification Rule. Furthermore, BUSINESS ASSOCIATE shall report to PROVIDER any security incident of which it becomes aware. This report shall be given to PROVIDER as soon as possible after BUSINESS ASSOCIATE discovers the impermissible use or disclosure but not more than _____ (___) days after the discovery. [45 CFR §164.504(e)(2)(ii)(C); *45 CFR §164.314(a)(2)(i)(C)*]

{Comment1: Subparagraph (d), above, is a required provision. The second sentence is optional. The Rule does not state how quickly the business associate should report, but the sooner the better. You may want to make the time period in