Bulletin

November 6, 2009

HIPAA compliance requirements

Blue Cross and Blue Shield of Minnesota and Blue Plus ("Blue Cross") considers its providers to be "business associates" under the federal Health Insurance Portability and Accountability Act (HIPAA). As business associates, providers are required to comply with certain provisions of HIPAA, which are currently spelled out in Blue Cross' provider agreements.

The recently enacted Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as incorporated in the American Recovery and Reinvestment Act of 2009 ("ARRA") amends HIPAA, placing additional responsibilities on business associates of covered entities. The law also imposes new breach notification requirements on covered entities for certain breaches of personal health information.

In order to be compliant with these new provisions, we are hereby amending the "HIPAA Compliance" section of your current Provider Service Agreement, effective February 17, 2010, as set forth below.

HIPAA Compliance. Pursuant to the federal Health Insurance Portability and Accountability Act (HIPAA) and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"), Provider agrees that it shall:

1. Not use or further disclose Protected Health Information (PHI) other than as permitted or required by this Agreement, and further agrees that it shall not use or further disclose PHI in a manner that would violate requirements of HIPAA and its implementing regulations (45 C.F.R. parts 160-64) ("HIPAA Regulations") or the HITECH Act.

2. Report to Blue Cross any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, and shall ensure that any agents, including any subcontractors, to whom it provides or from whom it receives PHI, agree to the same restrictions and conditions that apply to Provider with respect to such information.

3. Upon any termination of this Agreement, extend the protections of this Section to the PHI and limit further uses and disclosure to those purposes that make the return or destruction of the information infeasible.

4. Develop, implement, maintain and use appropriate administrative, technical and physical safeguards, in compliance with Social Security Act Sec. 1173(d) (42 U.S.C. Sec. 1320d-2(d)), 45 C.F.R. Sec. 164.530(c)) and any other implementing regulations issued by the U.S. Department of Health and Human Services.

Continued on back

Distribution: All participating providers
Bulletin P29-09

5. Upon receipt of notice from Blue Cross, promptly amend or permit Blue Cross access to amend any portion of the PHI which Provider created or received from Blue Cross so that Blue Cross may meet its amendment obligations under 45 C.F.R. Sec. 164.526.

6. With the exception of disclosures of PHI made for the purposes specified in 45 C.F.R 164.528(a)(1)(i)-(ix), document and report each disclosure, if any, Provider makes of any PHI Provider has created for Blue Cross or received from Blue Cross no later than five (5) days of the discovery of the disclosure. Upon Blue Cross' request, Provider shall perform a risk assessment to determine whether the disclosure poses a significant risk of financial, reputational or other harm to the individual(s) whose PHI was used or disclosed. Provider shall provide documentation relating to the risk assessment when Provider reports the disclosure to Blue Cross. If Blue Cross determines that notice to the individual(s), media or HHS is required, Provider shall be responsible for any and all costs relating to such notice. Provider shall cooperate with Blue Cross in investigating the disclosure and in meeting Blue Cross' obligations under the HITECH Act and any other security breach notification laws. In the event of any such disclosure, Provider shall:

a. Identify the nature of the non-permitted access, use or disclosure, including the date of the disclosure and the date of discovery of the disclosure;

b. Identify the PHI accessed, used or disclosed as part of the disclosure (e.g., full name, social security number, date of birth, etc.);

c. Identify who made the non-permitted access, use or disclosure and who received the non-permitted disclosure;

d. Identify what corrective action Provider took or will take to prevent further non-permitted access, uses or disclosures;

e. Identify what Provider did or will do to mitigate any deleterious effect of the non-permitted access, use or disclosure; and

f. Provide such other information, including a written report, as Blue Cross may reasonably request.

Provider acknowledgement

Provider acknowledges and agrees that in the event Provider breaches this Section, Blue Cross may either terminate this Agreement upon written notice to Provider and/or report such breach by Provider to the United States Department of Health and Human Services.

Questions?

If you have any questions, please contact provider service at (**651) 662-5200** or **1-800-262-0820**.