Genworth

Genworth Life & Annuity
Genworth Life
Genworth Life of New York

New Federal Privacy and Security Regulations for Long Term Care Insurance, Linked Benefit Products, and Medicare Supplement Insurance Producers

from Genworth Life and Annuity Insurance Company, Genworth Life Insurance Company and Genworth Life Insurance Company of New York†

†Only Genworth Life Insurance Company of New York is admitted in and conducts business in New York.

Dear Distribution Customer:

Background

You are receiving this because you are a Business Associate of Genworth Life Insurance Company, Genworth Life Insurance Company of New York, or Genworth Life and Annuity Insurance Company. On January 17, 2013, the U.S. Department of Health and Human Services ("HHS") issued a final rule ("Omnibus Rule"), which changed various aspects of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Omnibus Rule became effective on March 26, 2013, and Business Associates must comply with its requirements by September 23, 2013 (the "Compliance Date").

What has changed with the Omnibus Rule?

The Omnibus Rule confirmed many of the modifications to the privacy and security provisions of HIPAA set forth in the Interim Rules. Here are just a few of the important requirements of the Omnibus Rule:

1. The HIPAA privacy and security standards now apply directly to business associates – meaning that you, as a business associate, are now subject to the direct jurisdiction and enforcement of the Secretary of Health and Human Services.
2. Business associates, like you, must enter into Business Associate Agreements (BAA) with each of their business associates. In other words, you must enter into a Business Associate Agreement with each of your contractors or subcontractors who may have access to Protected Health Information (PHI), as that term is defined in HIPAA. You can find more information about BAA's, including sample provisions, at ***http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html***. Also, be aware that you may be subject to enforcement actions by HHS based on actions of your Business Associates.
3. The Omnibus Rule requires us to revise our Notice of Privacy Practices and to provide notice of those changes to our long term care insurance policyholders/certificate holders. We will begin sending notification to our policyholders/certificate holders about these changes shortly.

The Impact of these Changes on Your Business

With your current BAA, you already agreed to comply with certain specific requirements involving the privacy and security of PHI. The Omnibus Rule extends these requirements to you directly and you could be fined for your failure to comply. In addition, the Omnibus Rule obligates your company to follow the entire HIPAA Security Rule, including all of the requirements for technical, physical and administrative safeguards.

Generally, to be in compliance with the HIPAA Security Rule, a HIPAA covered entity (and now HIPAA business associates as well) must:

- Ensure confidentiality, integrity and availability of electronic protected health information created, received, maintained, and transmitted
- Protect against "reasonably anticipated threats or hazards" to "security or integrity" of this information
- Protect against "reasonably anticipated uses or disclosures" of this information that are not permitted under Privacy Rule
- Ensure compliance by your workforce

You should evaluate your security risks through a "risk assessment" and then implement an appropriate program to manage these risks. You may also wish to review the following regulatory links to confirm that you are in compliance. For added assurance, it is always a good idea to review your privacy and security program with your compliance and legal advisors and with information technology consultants who can assist you in developing an appropriate information security program.

- **http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf**
- **http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html**

Security Breach Notification

As a reminder, in addition to the requirements of the HIPAA Privacy and Security rules, HIPAA also requires notification to individuals and, in some circumstances, the Department of Health and Human Services and even the media, in the event of certain kinds of security breaches involving protected health information. **Your obligation** is to notify us of **any** potential security breach, so that we may determine whether there is a requirement to notify our insureds or otherwise respond. **Please make any initial report to the Genworth Fraud and Information Security Referral Team at 866 381.2906.** In addition, you should always act quickly to mitigate any potential harm from a potential security breach.

Security Best Practices

Because of the differences in size, sophistication and use of PHI, each business associate's privacy and security program for protecting and safeguarding PHI will vary – and the Security Rule makes clear that security compliance is not a "one size fits all" program. However, there are certain information security best practices that you should implement or consider, regardless of the size and structure of your organization. This is by no means an exhaustive list.

- Data Encryption – Encrypting your data protects the information and minimizes or eliminates certain notification obligations in the event of a security breach. Encryption is particularly important when using laptops, memory sticks, disks and similar devices that are easily lost or stolen. Furthermore, encryption software is more affordable than ever, so why wouldn't you protect yourself and your customers.
- Use physical and technological security safeguards as appropriate to protect personal information.
- Monitor employee or contractor access to information and remove access for former employees or contractors.
- Make employees aware of security and privacy policies through ongoing employee training and communications.
- Use intrusion detection technology and procedures to help ensure rapid detection of unauthorized accessto personal information.
- Implement an annual review process for all security plan(s) so that material changes in business practices, applicable laws, or potential methods effecting breach are incorporated into the plan.
- Adopt written procedures for internal and external notification of and evaluation of appropriate mitigation steps for security incidents that may involve unauthorized access to personal information.
- Utilize appropriate disposal practices for any kind of sensitive personal information, including where appropriate reasonable measures to:
    - Implement and monitor compliance with procedures that require burning, pulverizing, or shredding of paper containing consumer information so that it cannot be read or reconstructed.
    - Implement and monitor compliance with procedures that require destruction or erasure of electronic media containing consumer information so that it cannot be read or reconstructed.
    - Make sure that any service providers retained by you execute an appropriate subcontractor agreement incorporating the required HIPAA terms.

There are also many other resources available regarding effective information security.

We hope you find this information helpful and, as always, we appreciate the opportunity to meet the insurance andfinancial security needs of your customers.

Sincerely,

Your Genworth Sales Team