Sun Life and Health Insurance Company (U.S.)

New York Market Conduct Guide
Broker

September 2019

Table of Contents

Sun Life Commitment to Ethics and Compliance

Sun Life is proud of its history of delivering quality insurance products and services to its customers. Sun Life has a long-standing commitment to fair dealing and integrity that has contributed to its success. The ethical principles and compliance guidelines that are the foundation of Sun Life's compliance program are designed to help Sun Life, and you, fulfill our respective responsibilities to customers.

Peter Colli
Vice President & Chief Compliance Officer

Sun Life Commitment to Integrity

A guiding principle of Sun Life philosophy of management is Sun Life's commitment to fair dealing and integrity in the conduct of all aspects of its business. Acting with integrity is one of the values that serve as cornerstones to the vision and mission of Sun Life's U.S. operations. This value guides our policy of compliance with all applicable state and federal laws and regulations governing the marketing of insurance.

Our policy of compliance is not based solely on what the law requires us to do, but means that we look beyond the letter of the laws and regulations that govern our business and go the extra step of ensuring our practices address the underlying needs of customers. Employees and our distributors share accountability for understanding and following the ethical principles, compliance guidelines and procedures that help us fulfill our commitment to doing business the right way.

The way to protect our reputation is the same way we built it in the first place: by putting the needs of our customers first; by providing them with the information they need to make sound decisions; and, by offering products and services to meet their needs. Ethics and compliance work together to establish the sales practices that help us achieve these goals.

Sun Life Market Conduct Policy

Sun Life commitment to focus on the customer is fundamental to our success. In support of this commitment, Sun Life has developed Market Conduct Principles effective worldwide for its operations.

As Benefits professionals, you play a critical role with the customer. Your relationship with the customer offers opportunities to create appropriate expectations about our products and services and establish customer satisfaction, when these expectations are met.

The **Market Conduct Principles** are:

In the design and marketing of products and services, we will endeavor to:

- Assess both market and customer needs to create products and services that have value for the intended audience.
- Provide advertising and sales materials that are accurate, fair and clear.
- Periodically review the appropriateness of existing products' features and benefits.

In the recruitment, selection and training of representatives, we will endeavor to:

- Engage ethical and competent representatives who are knowledgeable about Sun Life's products and services.

In the sale of our products and services, we will endeavor to:

- Conduct business with integrity and fairness.
- Provide competent and customer-focused sales.
- Engage in fair competition.

In the ongoing servicing and support of customers who have purchased our products and services, we will endeavor to:

- Provide competent, timely and customer-focused service**.**
- Provide fair and expeditious handling of customer claims, complaints and disputes**.**
- Respect and protect our customers' personal information as outlined in Sun Life's Privacy Commitment**.**

Rebating/Inducement Policy

Rebating is considered an unethical inducement and is expressly illegal in nearly all states. Sun Life prohibits all methods of rebating in the sale of its products in all states. Also some states have published guidance in connection with "Value Added Services", which may be seen as a form of inducement.

Sales Practices

- Describe our products in clear, easy-to-understand terminology. Do not misrepresent the terms of our products.
- Conduct business with integrity and fairness.
- Avoid situations that give any appearance of a conflict of interest.
- Engage in fair competition.
- Do not disparage competitors, products or companies.
- Provide competent, timely and customer-focused service.
- Avoid all forms of "rebating" in the sale of our insurance products.
- Never sign a form on behalf of a customer.
- Never ask a client to sign a blank form; all forms must be completed before obtaining the signature.
- Manage the privacy requests of consumers in part by complying with federal and state telemarketing regulations. Protect customer nonpublic personal information in any form (e.g. paper, electronic, etc.) from unauthorized disclosure.
- Check the Sun Life sites to ensure required disclosure forms are completed when required.
- Adhere to state and federal "Do Not Call" regulations and other regulations pertaining to telephonic outreach to consumers, including autodialed or prerecorded telemarketing calls to wireless numbers and for prerecorded calls to residential lines.
- Know your customers. Verify their identity.

Sun Life and the Patriot Act Anti-Money Laundering Regulations

Please contact Paul Finnegan 781-446-6794 for information relating to the Sun Life Anti- Money Laundering Program.

Licensing, Appointments and Continuing Education

Representatives are required to be licensed as insurance brokers in the states where they will offer products. In addition, as brokers, you must be appointed by the applicable Sun Life companies in each state in which they offer our products. By example, if an enrollment occurs via telephone, fax, or on-line, the broker needs to be appointed in the state where the enrollee is located.

Since state insurance department regulations relative to the licensing and appointment of brokers may vary, brokers should become familiar with the requirements in any state in which they conduct business. While some states permit Sun Life to accept appointment paperwork simultaneously with the submission of business, other states, require that we appoint a broker **prior** to the solicitation of business. Some states have Continuing Education requirements that each broker must complete in order to maintain his/her license.

Errors and Omission Coverage

Sun Life requires that distributors who represent us must maintain certain Professional Liability coverage, at a minimum amount of $1 million, covering customary financial services errors and omissions liability. You must notify Sun Life if, at any time, coverage is terminated.

Your Duties as a Broker:

- Understand and comply with Sun Life licensing and appointment requirements.
- Solicit sales in states where you are appropriately licensed and appointed.
- Maintain your state insurance license.
- Complete any state mandated continuing education requirement.
- Fulfill continuing education requirements and maintain documentation supporting ongoing professional education.
- Maintain the errors and omission coverage required by Sun Life and have documentation that demonstrates proof of coverage. Brokers must provide satisfactory documentation of such coverage (e.g., a current Certificate of Insurance issued by the carrier) to Sun Life, on request.

Advertising and Sales Literature

Regulatory Obligations

As issuers of insurance products, the Sun Life companies are responsible for compliance with state insurance laws and regulations for advertising and sales literature. All brokers are subject to state insurance laws and regulations when engaged in the advertising and sales of insurance.

Sun Life's Advertising Review Requirements

Sun Life is committed to provide advertising and sales materials that are accurate, fair, balanced, and clear. All brokers selling our products must use only Sun Life-approved advertising and sales literature with clients. Accordingly, **any material that you create that refers to our companies or our products or any related services must be submitted to us for review and approval prior to use, including "Broker Use Only" items.** Although generic materials with no references to Sun Life or its products and services are ordinarily not subject to our approval, you are also reminded that state insurance regulations broadly define sales material to include any material used to create interest in an insurer or its products. It is your responsibility to comply with applicable regulatory standards, with respect to all such materials, including "Broker Use Only" items.

General Guidelines for Advertising and Sales Material:

- Disclose the benefits and limitations of our products
- Avoid unfair, incomplete, deceptive and misleading advertising
- Properly identify the product (e.g. life insurance policy)
- Refer to the actual product name at least once
- Use terminology from contracts when describing products
- Identify the issuing company when discussing a product
- Do not disparage competitors
- Avoid promissory statements
- Avoid use of absolute terms

Electronic advertising and sales literature that refer to Sun Life or its products is subject to the same review and approval process and applicable regulatory requirements (e.g. prospectus delivery for

variable insurance products) as printed materials. There are also additional considerations to take into account when utilizing the Internet to promote our products. For example, since the communication may appear in any number of jurisdictions, any product reference should state that the product may not be available in all states. When information that is subject to change is included, be sure to include an effective date, since it is difficult to control the future distribution of information transmitted over the Internet. Before establishing a link between any website and a website maintained by Sun Life, brokers must also obtain approval from us.

Social Media

Generally under state insurance regulations, most forms of Social media communications are subject to the same advertising rules. Consequently any use of social media is subject to the PUBS review process. Also, Sun Life has established Social Media Guidelines which must be followed.

E-mail Advertising

The Controlling of the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003) is a federal law that extends privacy rights beyond the customary definition of "consumer." In order to comply with CAN-SPAM with respect to recruiting ads, the law requires you (or your 3rd party vendor) to include the following in your email:

- Truthful information in the header fields of the email. Your name and e-mail address must be accurate and identify the person sending the email.
- Subject lines cannot be deceptive or misleading. They must state the true subject of the email.
- With all email solicitation, you must give the recipients the option to "opt-out" of receiving any future emails from you. You have ten days from receipt of an opt-out request to remove the requestor from your mailing list. The name of the opt-out individual cannot be sold or transferred.
- The email must be identified as an advertisement.

Use of Special Designations

A number of State Insurance Departments have recently adopted regulations concerning the use of designations or titles that may falsely imply that brokers have some special financial knowledge or training or that they are certified or qualified to provide specialized financial advice.

It is contrary to Sun Life's policy to use a designation or title that does not support our commitment to ethical Market Conduct. We want to remind all brokers that it is also your responsibility to follow the requirements of the states in which you operate your business. If a broker wants to use an advertisement that reflects a title or designation that appears to conflict with state regulation, we will require evidence to support the use of the designation (a copy of the course of study, examinations taken, etc.), as part of the PUBS review process.

Our review process is also designed to ensure that we fulfill our obligations under laws and regulations requiring ongoing maintenance of documentation regarding distribution of material, as well as copies of all advertising and sales material used to create interest in Sun Life and its products. You are reminded of the need to pull obsolete material from circulation and discontinue its use.

It is unlawful to use any marketing material that has not been properly approved. Failure to obtain approval of material requiring Sun Life approval could lead to the termination of a selling agreement or appointment and regulatory fines and sanctions. In addition, advertising approved by Sun Life may not be altered.

New York Regulation 34-A

New York has enacted rules governing the advertising of life insurance policies (known as Regulation 34-A). The intent of the Regulation is to ensure "truthful and adequate disclosure" and inclusion of "relevant information" in life insurance advertisements.

Definition of advertisement: Advertising, prepared by a broker or insurer, includes the following when used with the public as a means to "purchase, increase, modify, reinstate or retain" a life insurance policy: printed and published material, audio visual material, descriptive materials of an insurer, sales aides, and broker recruiting, training and educational materials.

Advertisement Requirements: Advertisements must be "truthful" and "not misleading" and must not "omit material information". Disclosures must not be confusing or misleading. There are guidelines for testimonials. These guidelines include the requirement that the testimonial reflects the opinion of the person in the testimonial, that the testimonial is an accurate representation of the individual's opinion and the disclosure of any financial gain on the part of the individual providing the testimonial. In addition, there are restrictions pertaining to certain words, including "free" and "no cost", and advertisements may not emphasize investment or tax features and forego or minimize the insurance aspects of the life insurance policy.

Your Duties as a Broker:

- Understand New York's Senior Designation Regulation (Regulation 199) and advertising requirements (New York Regulation 34-A).
- Understand and follow Sun Life's Advertising review process.
- Forward all customer and broker-use only materials intended to create interest in or to educate brokers or the public about any of the Sun Life's Companies, their products, or their services, to Sun Life for publication review (Pubs) and approval prior to use. Send advertising and sales materials that you would like reviewed to the applicable Sun Life Marketing Department.
- If material is approved with changes, the changes must be made prior to use of the material.
- You must not alter Pubs approved materials.
- Expired materials may not be used (Pubs approval for selling firm created materials is valid for one year).

Please contact the Compliance Department for additional information on the advertising and sales material review and approval process.

Needs Based Sales & Tax Advice

Sun Life endeavors to provide customer-focused sales. In keeping with our Market Conduct Policy, sales must be appropriate for each customer and based on the customer's needs.

Customers depend on your knowledge of products, markets, compliance rules, and industry standards. It is important that customers understand the basis of the recommendations you may make. Neither Sun Life nor any brokers are authorized to provide tax or legal advice to our customers on behalf of Sun Life. Because of the complexity of the tax and legal aspects of insurance in some circumstances, customers should be advised:

- to consult with their attorney for legal advice and guidance;
- to consult with their accountant or tax counsel to ensure understanding of IRS rules and regulations that may impact a buying decision.

Your Duties as a Broker:

- Ensure sales are consistent with customer needs and objectives and all related regulatory requirements.

Replacements

Before making any recommendation to replace a life insurance policy or annuity contract brokers should carefully consider the impact and consequences to the client of such a change. The recommendation to replace one policy or contract with another should be in the best interests of the customer and should be made only after carefully and fully disclosing to the customer the costs and impact of the change.

Your Duties as a Broker:

- Ensure you can demonstrate the replacement recommendation is in the best interest of the customer.
- Understand the definition of replacement.
- Understand and comply with New York's Regulation 60.

Privacy

Sun Life is committed to respecting and protecting our customers' personal information. You are required to protect our customers' nonpublic personal information (including financial and health information) in any form (e.g. paper, electronic, etc.) from unauthorized disclosure. In addition, many states have laws that require notification of the contract owner if there has been a breach of customers' personal information. You may be required to notify customers if there has been a breach of security of customer nonpublic information.

Your Duties as a Broker:

- Understand Sun Life's Privacy Policy
- Protect your customer's nonpublic personal information in any form (e.g. paper, electronic, etc.) from unauthorized disclosure at all times, and in states where applicable, appropriate electronic information encryption requirements should be followed.
- Nonpublic personal information of customers may only be shared with those who have a need to know for purposes of providing sales and service support.
- Securely dispose of customer nonpublic personal information in any form (placing customer information in locked recycling bins, shredding information or erasing or destroying electronic records).
- Notify the Privacy Officer immediately if you suspect that there has been a breach of our customers' confidential information or any improper disclosure of their personal information.

HIPAA Privacy

Sun Life is committed to maintaining the privacy of our customer's Protected Health Information ("PHI") under the 1996 Health Insurance Portability and Accountability Act ("HIPAA). PHI is broadly defined as any individually identifiable oral or recorded information related to the past, present or future physical or mental health of an individual. Certain products offered by Sun Life (e.g. group dental, accelerated benefit for long-term care expenses rider) are subject to the HIPAA Privacy Rule. All Brokers (and their staff) who offer any of these products are required to follow the Sun Life Broker Policy. By offering or selling any of these products to our customers you are agreeing to comply with the provisions of the Sun Life Broker Policy.

Your Duties as a Broker:

- Understand your obligations under the Sun Life Broker Policy (Refer to Broker Policy in this Guide)
- Implement and maintain appropriate administrative, technical and physical safeguards to protect PHI against unauthorized disclosure

- Protect against any anticipated threats or hazards to the security or integrity of the PHI
- Protect against any unauthorized use of or access to PHI which could result in substantial harm or inconvenience to any customer
- Notify the HIPAA Privacy Officer immediately if you suspect that there has been a breach of our customers' confidential information or any improper disclosure of PHI.

New York DFS Cyber Security Regulation – 23 NYCRR 500

The regulation required all DFS regulated entities, subject to certain exemptions, to adopt the core requirements of a cybersecurity program, including a cybersecurity policy, effective access privileges, cybersecurity risk assessments, and training and monitoring for all authorized users, among other requirements. The regulation also requires the establishment of governance processes to ensure senior attention to these important protections. The final effective date for the regulation will be March 1, 2019, by which time, under section 500.11, DFS regulated entities are required to have written policies and procedures that are based on a risk assessment to ensure the security of nonpublic information and information systems that are accessed or held by third party service providers.

Accordingly, by March 1, 2019 all banks, insurance companies, and financial services institutions and licensees regulated by DFS will be required to have a robust cybersecurity program in place that is designed to protect consumers' private data; a written policy or policies that are approved by the Board of Directors or a Senior Officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial service industry including encryption and multifactor authentication. The regulations sets forth certain limited exemptions, many of which will require certain cybersecurity programs and practices.

Your Duties as a Broker:

- Understand your responsibilities and accountabilities under the New York Department of Financial Services Cyber Security Regulation
- Understand your responsibilities and accountabilities under Sun Life's Cyber Security Program, including policies and procedures.
- Protect your client's personal and/or Nonpublic information and Sun Life's data, in any form (e.g. paper, electronic, etc.) from unauthorized disclosure at all times.
- Securely dispose of client nonpublic personal information in any form (placing client information in locked recycling bins, shredding information or erasing or destroying electronic records).
- Notify the Privacy Officer immediately if you suspect that there has been a cyber security breach involving your client's and/or company's information.

Complaint Handling

Sun Life endeavors to provide fair and expeditious handling of customer complaints. Complaints about Sun Life products and services are a means of measuring the areas in which we need to improve. Therefore, it is critical that Sun Life monitor complaints about the Sun Life Companies, its products and services by customers, policyholders, regulatory agencies or competitors.

Sun Life and our distributors are required by insurance laws and regulations to maintain complaint handling and reporting procedures. Since Sun Life is required to address complaints within time frames established by the Sun Life Companies' procedures and applicable regulations (e.g., state insurance laws), we remind brokers of their responsibility to **promptly notify us of any complaint.**

Definition of a Complaint

Generally, a complaint is defined as any communication, whether oral or written, which expresses either a grievance or dissatisfaction with Sun Life's products, services or procedures or with the activities of brokers in connection with the sale, distribution, or servicing of Sun Life products, or related services.

Sun Life must keep a register of all such complaints, which may come from any number of sources, including, among other, policyholders, brokers, service providers, state insurance departments or other regulatory agencies. Written complaints received from the state insurance departments or other regulatory agencies must be date stamped and forwarded immediately with all supporting documents to Sun Life, Compliance Division SC 3093, 110 Worcester Street, Wellesley Hills, MA 02481 or complaints.mailbox@sunlife.com. Electronic complaints received from the state insurance department or other regulatory agencies may be forwarded to complaints.mailbox@sunlife.com. All other written complaints should be handled according to the internal guidelines of your department.

To assist us in this process, we may request documents and records from you. Additionally, we may request that a broker and his or her firm provide us with written statements responding to the allegations raised in a complaint. We will work with you to determine the appropriate course of action, if any, to resolve the matter.

Sun Life may also request documents and records related to the offer and sale of our products and services while conducting investigations or reviews, either as a result of regulatory inquiries or as part of our compliance monitoring. In addition to maintaining such records in accordance with applicable laws and regulations that apply to your business, Sun Life relies on your full cooperation in sharing copies of your documents and records to fulfill our respective responsibilities to the purchasers of our products.

Your Duties as a Broker:

- **Immediately report complaints to Sun Life, Compliance Division SC3093, 110 Worcester Street, Wellesley Hills, MA 02481 or to complaints.mailbox@sunlife.com.**
- If a client makes an oral complaint, but declines to document the complaint in writing, document the grievance and forward to Sun Life.
- Work with Sun Life to ensure the fair and expeditious handling of a complaint.
- You must not offer settlements in an effort to resolve complaints.
- Immediately notify Sun Life's Law Department upon receipt or notification of a lawsuit against Sun Life or Broker pertaining to his or her representation of Sun Life, a subpoena for company information or a judgment, garnishment, lien or forfeiture order.
- Respond to requests from Home Office personnel within established time frame in order to promptly resolve the complaint.
- Ensure that responses are complete and documented as best as they can be.

Please contact Debby Webster AVP, Compliance, at debby.webster@sunlife.com for additional information about these procedures.

Fraud Reporting and Investigation

Sun Life is committed to fair dealing and integrity in the conduct of its business. It expects all employees and representatives, including brokers, to share this commitment, and to have responsibility for their own actions, as well as associated staff. Sun Life has established a fraud reporting and investigation framework for reporting and investigating suspected fraudulent acts or omissions of any employees or representatives, or by any third parties. Any suspected fraud should be reported immediately. If, after investigation, it is determined that a fraud has occurred, the person(s) involved will be subject to disciplinary action, including termination.

How to Report Fraud:

Any suspicions of fraud should be reported immediately to Sun Life, by calling 1-800-481-6966.

Your Duties as a Broker:

- If you suspect a fraudulent act has occurred, it should be reported immediately, see fraud reporting, above
- Cooperate with any Sun Life investigation

Maintaining Customer Records

A well-documented client file, whether in paper form or electronic, should contain information that tracks the actions you take in your work with prospects and clients, including fact-finding data, analyses and other information that establishes the basis for the amount and type of product sold.

In addition, clients files should include: copies of all correspondence with clients and/or their advisors; case notes and a log of telephone calls; documentation that supports the determination of customers' insurance needs.

Your Duties as a Broker:

- Effectively document your sales and service client communications and practices.
- Secure client nonpublic personal information to prevent unauthorized disclosure of this information.

Service

Premium Payments

As a matter of Sun Life policy, Sun Life does not allow brokers to use their own funds (including checks or wire transfers) to make payments on behalf of their clients, nor to collect premium payments from clients.

Address of Record

Brokers' addresses may not be the address of record for a customer.

Brokers Serving as Trustees:

From time to time, brokers may be asked to serve as trustee on behalf of their clients. There are a number of reasons why you should not accept that role.

- A trustee is held to a higher standard than most financial services representatives - service and advice must always be in the clients' best interests, even at the cost of a broker's own best interest. In addition, as a fiduciary, trustees are responsible for exercising scrupulous good faith and candor on behalf of clients. Disclosure requirements for trustees are, therefore, stringent and any actual or potential conflicts of interest with a client must be disclosed at the outset of a relationship. Disclosure should include not only how the product will work and the risk involved, but also a broker's relationship with product issuers and/or broker-dealers, and the method and amount of compensation from those entities.
- A broker's role as agent or broker creates an inherent conflict of interest with his or her role as trustee. If a dispute arises between the client and the issuer or dealer in which the broker is implicated, the broker may have an interest in defending a role as agent or broker that conflicts with his or her responsibilities as trustee to pursue the client's competing interests in the dispute.
- It may not be permitted in some states, e.g., California. Given the inherent conflicts between the broker's roles as trustee and agent or broker, Sun Life does not allow brokers to assume the trustee role on behalf of clients.

Compliance Responsibilities

Under the terms of our distribution and selling agreements, all brokers are responsible for compliance with applicable laws and regulations.

Sun Life will assist you in meeting these compliance responsibilities by providing information and resources designed to help you understand our products, appropriate markets and uses, as well as compliance monitoring of sales practices, e.g. monitoring of replacement transactions. If you have any compliance questions, we encourage you to call the Compliance Department.

Disclosure of Compensation

New York Regulation 194 ("194") requires Brokers, effective January 1, 2011, disclose to clients information about the nature and amount of compensation to be received as a result of a transaction.

"Compensation" under 194 is defined broadly to include money, credits, loans, interest on premiums, forgiveness of principal or interest, trips, prizes or gifts, whether paid as commission or otherwise. The only exception noted is insurer "logo" items having an aggregate value of less than $100 per year. No particular format for this disclosure is dictated by the rule, or the related Circular Letter.

194 requires Brokers conducting business in the state of NY (whether on a resident or non resident basis) to prominently disclose, at or before the time of application:

1. Their role in the transaction
2. Whether they receive compensation based, in whole or part, on the sale
3. That the compensation may vary based on factors such as value of business
4. That the broker will provide specific details (described below) upon request

The details about the broker's compensation must include:

1. their known compensation expressed as either: a total dollar amount, the total commissions expressed as a percentage of annual premium or, the compensation received expressed as a percentage of premiums paid over the expected duration of the policy or contract. The broker must also offer an explanation that most of the compensation will be received in the first year, if that is the case.

2. a "reasonable estimate" of their other expected compensation, even though the amount is unknown at that time, such as bonuses based on volume, profitability or retention, or some other form of contingency.

It is the obligation of the broker to maintain records for three years, certifying that the appropriate disclosures have been made.

Your duties as a Broker:

- Make all required compensation disclosures to clients
- Maintain records of disclosures in client files

Important Information about Sun Life's Compliance Program

This manual communicates the principles and policies that Sun Life and Health Insurance Company (U.S.) a member of the Sun Life group of companies, has adopted to maintain compliance with laws, regulations and the terms of our distributor agreements. Brokers appointed with Sun Life Assurance Company of Canada are advised to refer to the Market Conduct Guide for Sun Life Assurance Company of Canada. All appointed brokers, at all levels, are subject to this manual. The manual is designed to serve as a reference source for the key roles and responsibilities that we share in meeting the needs of our mutual customers. While it is not an all-inclusive source of compliance requirements, familiarity with these key compliance guidelines can help minimize the risks associated with client complaints, regulatory problems and adverse publicity. This manual is not intended, however, to amend or modify any of the terms of your distribution/selling agreement(s), nor to serve as a substitute for your thorough understanding of all laws, regulations and Sun Life policies pertaining to your activities. Brokers are subject to Company sanctions for violations of Sun Life compliance guidelines and policies outlined in this Market Conduct Guide. Brokers may report potential violations of Sun Life's compliance guidelines and policies outlined in this Market Conduct Guide to Peter Colli, Vice President and Chief Compliance Officer.

The terms "Sun Life," "we," "our," and "us" as used in this manual refer to Sun Life and Health Insurance Company (U.S.) and all affiliated companies. As policies and procedures described in this manual are revised in response to legal and regulatory developments, we reserve the right to amend or modify this material at any time.

Sun Life

Broker Policy

New York Department of Financial Services Cyber Security Regulation – 23 NYCRR 500

Section 500.00 Introduction:

The New York State Department of Financial Services ("DFS") has been closely monitoring the evergrowing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Section 500.01 Definitions:

For purposes of this Part only, the following definitions shall apply:

(a) Affiliate means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.
(b) Authorized User means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) Covered Entity means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(d) Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information system

(e) Information System means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(f) Multi-Factor Authentication means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(g) Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

(h) Penetration Testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(i) Person means any individual or any non-governmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency or association.

(j) Publicly Available Information means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) Risk Assessment means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.
(l) Risk-Based Authentication means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.
(m) Senior Officer(s) means the senior individual or individuals (acting collectively or as a committee)

responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) Third Party Service Provider(s) means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

Section 500.02 Cybersecurity Program.

(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.
(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:
(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;
(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;
(3) detect Cybersecurity Events;
(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;
(5) recover from Cybersecurity Events and restore normal operations and services; and
(6) fulfill applicable regulatory reporting obligations.
(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.
(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Section 500.03 Cybersecurity Policy.

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee there of) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information

Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;
(b) data governance and classification;
(c) asset inventory and device management;
(d) access controls and identity management;
(e) business continuity and disaster recovery planning and resources;
(f) systems operations and availability concerns;
(g) systems and network security;
(h) systems and network monitoring;
(i) systems and application development and quality assurance;
(j) physical security and environmental controls;
(k) customer data privacy;
(l) vendor and Third Party Service Provider management;
(m) risk assessment; and (n) incident response.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO").

The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:
(1) retain responsibility for compliance with this Part;
(2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and
(3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider:

(1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;
(2) the Covered Entity's cybersecurity policies and procedures;
(3) material cybersecurity risks to the Covered Entity;
(4) overall effectiveness of the Covered Entity's cybersecurity program; and
(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic

Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail.

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity. Section 500.09 Risk Assessment.

Section 500.09 Risk Assessment.

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular

risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of

the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 500.14 Training and Monitoring.

As part of its cybersecurity program, each Covered Entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and (b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity

shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

Section 500.18 Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

(a) Limited Exemption. Each Covered Entity with:

(1) fewer than 10 employees, including any independent contractors, of the Covered Entity and its Affiliates located in New York or responsible for business of the covered entity, or

(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or

(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 500.20 Enforcement.

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

Section 500.21 Effective Date.

This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

Section 500.22 Transitional Periods.

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.
(b) The following provisions shall include additional transitional periods. Covered Entities shall have:
(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.
(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.
(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

Section 500.23 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

Health Insurance Portability and Accountability Act, "HIPPA"

Pursuant to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations at 45 C.F.R Parts 160-164 (collectively "HIPAA") Sun Life Assurance Company of Canada, Sun Life and Health Insurance Company (U.S.) and certain other affiliates (collectively "the Company") and Brokers are required to regulate the use and disclosure of certain individually identifiable information. Insurance brokers and other distributors contracted with or appointed by the Company to sell products subject to HIPAA who are provided PHI by on behalf of the Company for the purpose of selling or administering insurance coverage qualify as Brokers and are required to comply with the provisions of this Broker Policy (''Policy").

This Policy is limited to the extent that the Company is a Covered Entity as defined below. This Policy constitutes a Company policy, rule, guideline, or any other form of statement which creates an obligation under applicable broker agreements or conditions of employment. Unless otherwise stated, this Policy shall apply to all services between the Broker and Sun Life.

The broker has access to Protected Health Information ("PHI"), through its services in providing licensed insurance sales and brokerage.

HIPAA requires written agreements or arrangements with brokers to regulate the use and disclosure of Protected Health Information; Brokers also have independent compliance obligations under the Privacy Standards and Security Standards.

In order to disclose and protect information given to the Broker, some of which may constitute PHI, the Broker and Sun Life agree to the following:

1. Definitions. All terms that are used but not otherwise defined in this Policy shall have the meaning specified under HIPAA, including its statute, regulations and other official government guidance. In addition to the terms in the Agreement, the following terms when capitalized will have this meaning:

   a. Breach. "Breach" shall have the same meaning as the term "Breach" in 45 CFR § 164.402.

   b. Broker. "Broker" shall have the meaning provided for in 45 CFR § 160.103.

   c. Covered Entity. "Covered Entity" shall mean Sun Life Assurance Company of Canada, and Sun Life and Health Insurance Company (U.S.).

   d. Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR § 164.501.

e. Electronic Health Record. "Electronic Health Record" shall have the same meaning as the term "electronic protected health information" in American Recovery and Reinvestment Act of 2009,§ 13400(5).

f. Electronic Protected Health Information. "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103.

g. Electronic Transactions Rule. "Electronic Transactions Rule" shall mean the final regulations issued by HHS concerning standard transactions and code sets under 45 CFR Parts 160 and 162.

h. HHS. "HHS" shall mean the Department of Health and Human Services.

i. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, subparts A and E.

j. Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information created or received by Broker from or on behalf of Covered Entity.

k. Required By Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

l. Security Incident. "Security Incident" shall have the same meaning as the term "securing incident" in 45 CFR § 164.304.

m. Security Rule. "Security Rule" shall mean the Security Standards and Implementation Specifications at 45 CFR Parts 160 and 164, subpa11C.

n. Transaction. 'Transaction" shall have the meaning given the term "transaction" in 45 CFR § 160.103.

o. Unsecured Protected Health Information. "Unsecured Protected Health Information" shall have the meaning given the term "unsecured protected health information" in 45 CFR § 164.402.

2. Broker Operations. Broker of Sun Life, agrees to comply with all applicable privacy and security laws and regulations, including those set forth in the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. 160, 162 and 164) ("HIPAA"), as may be amended from time to time, and any other applicable privacy and security law as a Broker of Sun Life.

3. Safeguarding Privacy and Security of Protected Health Information

a. Permitted Uses and Disclosures. Broker is permitted to use and disclose Protected Health Information that it creates or receives on Covered Entity's behalf or receives from Covered Entity (or another broker of Covered Entity) and to request Protected Health Information on Covered Entity's behalf (collectively, "Covered Entity's Protected Health Information") only:

i. Functions and Activities on Covered Entity's Behalf. To act as the agent of record for group insurance plans.

ii. Broker Operations. For Broker/s proper management and administration or to carry out Broker's legal responsibilities, provided that, with respect to disclosure of Covered Entity's Protected Health Information, either:

1. The disclosure is Required by Law; or

2. Broker obtains reasonable assurance from any person or entity to which broker will disclose Covered Entity's Protected Health Information that the person or entity will: (1) Hold Covered Entity's Protected Health Information in confidence and use or further disclose Covered Entity's Protected Health Information only for the purpose for which broker disclosed Covered Entity's Protected Health Information to the person or entity or as Required by Law; and (2) Promptly notify broker (who will in turn notify Covered Entity in accordance with the breach notification provisions) of any instance of which the person or entity becomes aware in which the confidentiality of Covered Entity's Protected Health Information was breached.

3. Minimum Necessary. Broker will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of Covered Entity's Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, consistent with this Policy and the Privacy Rule, except that Broker will not be obligated to comply with this minimum-necessary limitation if neither Broker nor Covered Entity is required to limit its use, disclosure or request to the minimum necessary. Broker and Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), passed as part of the American Recovery and Reinvestment Act of 2009, and government guidance on the definition.

b. Prohibition on Unauthorized Use or Disclosure. Broker will neither use nor disclose Covered Entity's Protected Health Information, except as permitted or required by this Agreement or in writing by Covered Entity or as Required by Law. This Agreement does not authorize Broker to use or disclose Covered Entity's Protected Health Information in a manner that will violate the Privacy Rule if done by Covered Entity.

c. Information Safeguards. Broker will provide the following Information Safeguards:

1. Privacy of Covered Entity's Protected Health Information. Broker will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards (''Safeguards") to protect the privacy of Covered Entity's Protected Health Information. Safeguards must reasonably protect Covered Entity's Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this Agreement.

2. Security of Covered Entity's Electronic Protected Health Information. Broker will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of, and to prevent non-permitted or violating use or disclosure of, electronic Protected Health Information created, transmitted, maintained or received in connection with the services, functions, and/or transactions to be provided under this Policy or the Service Agreement, consistent with the requirements of the HIPAA Security Rule, and will comply with all requirements of such Security Rule. Broker will document and keep these Safeguards current. Broker agrees to provide training to its workforce as required by 45 CFR 164.530. Broker will comply with any additional requirements as requested by Covered Entity.

d. Subcontractors and Agents. Broker will require any of its subcontractors and agents, to which Broker is permitted by this Policy or in writing by Covered Entity to disclose Covered Entity's Protected Health Information *and/or* Electronic Protected Health Information, to provide reasonable assurance that such subcontractor or agent will comply with the same privacy and security safeguard obligations with respect to Covered Entity's Protected Health Information and/or Electronic Protected Health Information that are applicable to Broker under this Policy.

e. Prohibition on Sale of Records. As of the effective date specified by HHS in final regulations to be issued on this topic, Broker shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual unless the Covered Entity or Broker obtained from the individual, in accordance with 45 CFR § 164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that individual, except as otherwise allowed under the HITECH Act.

f. Penalties for Non-compliance. Broker acknowledges that it is subject to civil and criminal enforcement for failure to comply with the privacy rule and security rule, as amended by the HITECH Act.

4. Compliance with Electronic Transactions Rule. If Broker conducts in whole or part electronic Transactions on behalf of Covered Entity for which HHS has established standards, Broker will comply, and will require any subcontractor or agent it involves with the conduct of such Transactions to comply, with each applicable requirement of the Electronic Transactions Rule. Broker Associate shall also comply with the National Provider Identifier requirements, if and to the extent applicable.

5. Individual Rights. Broker will maintain the following rights for individuals:

a. Access. Broker will, within twenty (20) calendar days following Covered Entity's request, make available, in a time and manner required by the Privacy Rule, and in a Designated Record Set where permitted and appropriate, Covered Entity's Protected Health Information

about the individual that is in Broker's custody or control to Covered Entity or, at Covered Entity's direction, to an individual (or the individual's personal representative) for inspection and obtaining copies so that Covered Entity may meet its access obligations under 45 CFR § 164.524. Effective as of the date specified by HHS, if the Protected Health Information is held in an Electronic Health Record, then the individual shall have a right to obtain from Business Associate a copy of such information in an electronic format.

Broker shall provide such a copy to Covered Entity or, alternatively, to the individual directly, if such alternative choice is clearly, conspicuously, and specifically made by the individual or Covered Entity.

b. Amendment. Broker will, upon receipt of written notice from Covered Entity, promptly amend or permit Covered Entity access to amend any portion of Covered Entity's Protected Health Information, so that Covered Entity may meet its amendment obligations under 45 CFR § 164.526.

c. Disclosure Accounting. Broker will facilitate Covered Entity's ability to meet its disclosure accounting obligations under 45 CFR § 164.528 in the following manner:

i. Disclosures Subject to Accounting. Broker will record the information specified below ("Disclosure Information") for each disclosure of Covered Entity's Protected Health Information, not excepted from disclosure accounting as specified below, that Broker makes to Covered Entity or to a third party.

ii. Disclosures Not Subject to Accounting. Broker will not be obligated to record Disclosure Information or otherwise account for disclosures of Covered Entity's Protected Health Information if Covered Entity need not account for such disclosures.

iii. Disclosure Information. With respect to any disclosure by Broker of Covered Entity's Protected Health Information that is not excepted from disclosure accounting, Broker will record the following Disclosure Information as applicable to the type of accountable disclosure made:

1. Disclosure Information Generally. Except for repetitive disclosures of Covered Entity's Protected Health Information as specified below, the Disclosure Information that Broker must record for each accountable disclosure is (i) the disclosure date, (ii) the name and (if known) address of the entity to which Broker made the disclosure, (iii) a brief description of Covered Entity's Protected Health Information disclosed, and (iv) a brief statement of the purpose of the disclosure.

2. Disclosure Information for Repetitive Disclosures. For repetitive disclosures of Covered Entity's Protected Health Information that Business Associate makes for a single purpose to the same person or entity (including Covered Entity), the Disclosure Information that Broker must record is either the Disclosure Information specified above for each accountable disclosure, or

(i) the Disclosure Information specified above for the first of the repetitive accountable disclosures;

(ii) the frequency, periodicity, or number of the repetitive accountable disclosures; and

(iii) the date of the last of the repetitive accountable disclosures (iv) Availability of Disclosure Information. Broker will maintain the Disclosure Information for at least six (6) years following the date of the accountable disclosure to which the Disclosure Information relates (Three (3) years for disclosures related to an Electronic Health Record, starting with the date specified by HHS).

Broker will make the Disclosure Information available to Covered Entity within twenty (20) calendar days following Covered Entity's request for such Disclosure Information to comply with an individual's request for disclosure accounting. Effective as of the date specified by HHS, with respect to disclosures related to an Electronic Health Record, Broker shall provide the accounting directly to an individual making such a disclosure request, if a direct response is requested by the individual.

d. Restriction Agreements and Confidential Communications. Broker will comply with any agreement that Covered Entity makes that either (i) restricts use or disclosure of Covered Entity's Protected Health Information pursuant to 45 CFR § 164.522(a), or (ii) requires confidential communication about Covered Entity's Protected Health Information pursuant to 45 CFR § 164.522(b), provided that Covered Entity notifies Broker in writing of the restriction or confidential communication obligations that Broker must follow. Covered Entity will promptly notify Broker in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Broker whether any of Covered Entity's Protected Health Information will remain subject to the terms of the restriction agreement. Effective February 17, 2010 (or such other date specified as the effective date by HHS), Broker will comply with any restriction request if (i) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (ii) the Protected Health Information pertains solely to a health care item or service for which the health care provider involved has been paid out-of-pocket in full.

6. Breaches and Security Incidents. Breaches and Security Incidents shall be handled in the following manner:

a. Reporting. Broker will report Breaches, suspected Breaches and Security Incidents as follows:

1. Privacy or Security Breach. Broker will report promptly to Covered Entity any use or disclosure of Covered Entity's Protected Health Information not provided for by this Agreement along with any Breach or suspected Breach of Covered Entity's Unsecured Protected Health Information. Broker will treat the Breach as being discovered in accordance with 45 CFR § 164.410. Business Associate also shall notify Covered Entity within ten days of any Breach of "Undisclosed Protected Health Information" as defined by the Breach Notification Rule set forth at 45 CFR Part 164 Subpart D. Any such report shall include the identification (if known) of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Further, Broker's notification shall at least:

- Identify the nature of the non-permitted use or disclosure or other breach;
- Identify the PHI used, accessed or disclosed;
- Identify who made the non-permitted use or received the non-permitted disclosure;
- Identify what corrective action Broker took or will take to prevent further non-permitted uses or disclosures;

- Identify what Broker did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and
- Provide such other information, including a written report, as Covered Entity may reasonably request.

ii. Security Incidents. Broker will report to Covered Entity any attempted or successful (A) unauthorized access, use, disclosure, modification, or destruction of Covered Entity's Electronic Protected Health Information or (B) interference with Broker's system operations in Broker's information systems, of which Broker becomes aware. Broker will make this report upon request, except if any such security incident resulted in a disclosure not permitted by this Agreement or Breach of Covered Entity's Unsecured Protected Health Information, Broker will make the report in accordance with the provisions set forth in the paragraph above.

7. Term and Termination.

a. Term. The term of this Policy shall terminate when all Protected Health Information provided by Covered Entity to Broker, or created or received by Broker on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

b. Right to Terminate for Cause. Covered Entity may terminate Policy if it determines, in its sole discretion, that Broker has breached any provision of this Policy, and upon written notice to Broker of the breach, Broker fails to cure the breach within thirty (30) calendar days after receipt of the notice. *Any* such termination will be effective immediately or at such other date specified in Covered Entity's notice of termination.

c. Return or Destruction of Covered Entity's Protected Health Information as Feasible. Upon termination or other conclusion of this Policy, Broker will, if feasible, return to Covered Entity or destroy all of Covered Entity's Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of Covered Entity's Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of the Broker. Further, Broker shall require any such sub-contractor or agent to certify to Broker that it returned to Broker (so that Broker may return it to the Covered Entity) or destroyed all such information which could be returned or destroyed. Broker will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of this Policy.

d. Procedure When Return or Destruction Is Not Feasible. Broker will identify any of Covered Entity's Protected Health Information, including any that Broker has disclosed to subcontractors or agents as permitted under this Policy, that cannot feasibly be returned to Covered Entity or destroyed and explain why return or destruction is infeasible. Broker will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Broker will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of the termination or other conclusion of Policy.

e. Continuing Privacy and Security Obligation. Broker's obligation to protect the privacy and safeguard the security of Covered Entity's Protected Health Information as specified in this Policy will be continuous and survive termination or other conclusion of this Policy, or the underlying Agreement.

8. General Provisions.

a. Inspection of Internal Practices, Books, and Records. Broker will make its internal practices, books, and records relating to its use and disclosure of Covered Entity's Protected Health Information, and its policies and procedures and related documentation pursuant to the Security Rule, available to Covered Entity and to HHS to determine compliance with the Privacy Rule and Security Rule.

b. Amendment to Policy. Upon the compliance date of any final regulation or amendment to final regulation promulgated by HHS that affects Broker or Covered Entity's obligations under this Policy, this Policy will automatically amend such that the obligations imposed on Broker or Covered Entity remain in compliance with the final regulation or amendment to final regulation.

c. No Third-Party Beneficiaries. Nothing in this Policy shall be construed as creating any rights or benefits to any third parties.

d. Interpretation. Any ambiguity in the Policy shall be resolved to permit Covered Entity and Broker to comply with the applicable requirements under HIPAA.

e. Indemnification. *[Add if there is nothing specific in the underlying agreement]* The Parties agree to indemnify each other and each respective director, officer, employee and agent, from and against all actions, liabilities damages, injuries, judgments and external expenses including all incidental expenses in connection with such liabilities, obligations, claims or actions based upon or arising out of damages sustained in connection with the performance of this Policy, brought, alleged or incurred and based upon:

i. Any alleged or actual violation of any law or regulation by either Party or any of its Affiliates or representatives; or

ii. The gross negligence or willful misconduct of either Party or any of its Affiliates or representatives; or

iii. The improper or illegal use or disclosure of, whether negligent or willful, of any PHI.

f. Subpoenas. Broker agrees to provide notice to Covered Entity of any subpoena or other legal process seeking PHI received from or created on behalf of Covered Entity or its affiliates. Such notice shall be provided within forty-eight (48) hours of receipt.

g. State Law. Where the mandatory terms of the HIPAA Privacy or Security Rule conflict with obligations imposed under state law, the Federal law shall govern.

h. Assignment. Upon written notice to Broker, Covered Entity shall have the right to assign this Policy to any successor or affiliate company. Broker may not assign this Policy without prior written consent, which will not be unreasonably withheld.

1. Paragraph Headings. Paragraph headings are for reference purposes only and shall not affect in any way the meaning or interpretation of this Policy.

J. Recitals. The recitals contained in the preamble to this Policy are made a part of the terms, provisions and conditions, and shall be binding on the parties as if fully set forth within the Policy.