McDermott Will & Emery

Fiduciary Issues and Data Privacy
Is Your Plan Data Really Safe?

March 23, 2016

Ann Killilea
akillilea@mwe.com
+1 617 535 3933

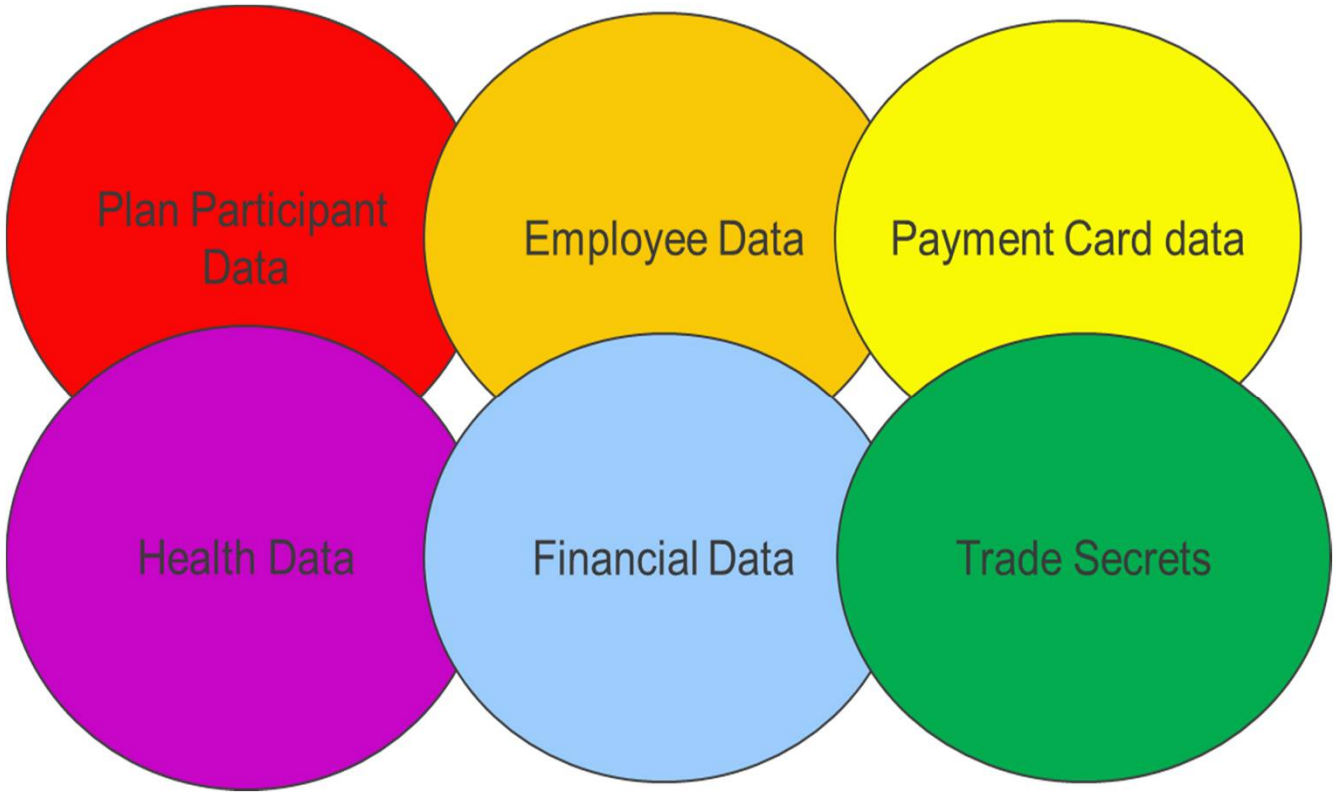
Andrew C. Liazos
aliazos@mwe.com
+1 617 535 4038

McDermott Will & Emery

What is Data Privacy?

It's All About The Data

McDermott Will & Emery



Personally Identifiable Information (PII) – U.S. State Laws

McDermott Will & Emery

- Definition of PII triggers breach notification requirements in 49 U.S. jurisdictions (47 states, DC and Puerto Rico)
- Definitions broadening traditional notions of regulated personal data
- Primarily designed to cover information that can be used for identity theft
- Name Plus model: Name or first initial and last name, in combination with 1 of 3 types of information: (1) social security number; (2) driver's license or state id number; or, (3) financial account number or credit card number, with or without any required code/number/password that would permit access to a financial account. (e.g., Mass.)
- PII expanding to include health information (e.g., Texas); health insurance information (e.g., Cal.); employee id number (e.g., North Dakota); IP address (e.g., Cal.) and more

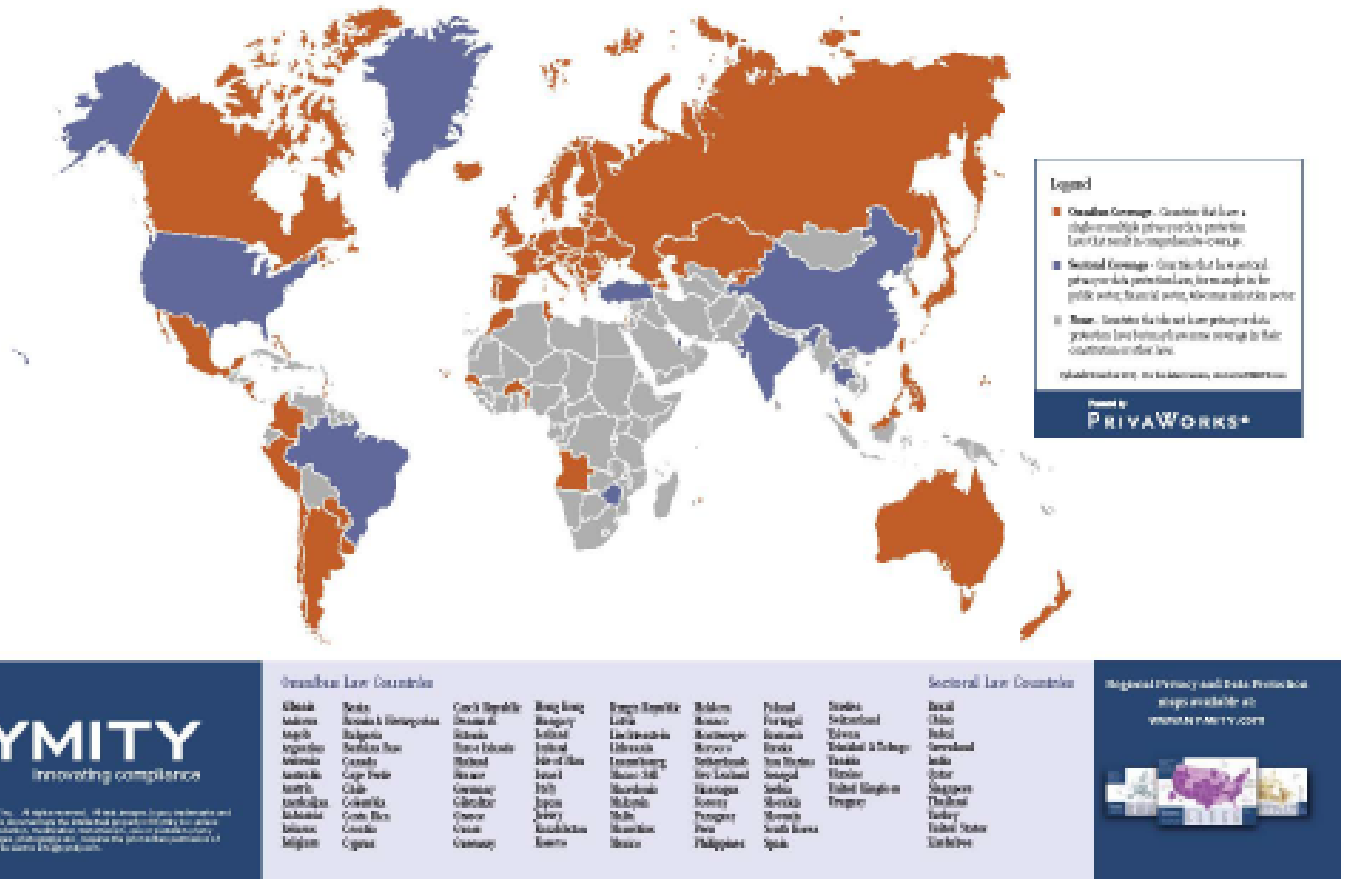
Skate to Where the Puck is Going

McDermott Will & Emery

- EU: Data relating to an identified or identifiable natural person
- State law PII definitions are increasingly adding new data elements
- FTC Commissioner: The distinction between PII and non-PII is blurring
- Proposed federal legislation seeks to harmonize existing state breach notification laws – broader than the Name Plus model
- Building corporate privacy management programs involves use of the broadest possible definitions as a high water mark

Data Privacy is Highly Regulated Worldwide

McDermott Will & Emery



A Patchwork of Non-ERISA Laws Applies to PII

McDermott Will & Emery

- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transactions Act (FACTA)
- Gramm-Leach-Bliley Act (GLBA)
- State laws
  - Identity Theft/Consumer Report Security Freeze Laws
  - Security Breach Notification Law
  - Protection of social security numbers
  - Disposal of personal information
- EU Data Protection Directive

State Laws May Be Implicated

McDermott Will & Emery

- 47 states, DC and US territories have state breach notifications laws
- Laws vary between jurisdictions
- Some states include health information within definition of PII; all include SSNs
- Some states exempt entities who comply with HIPAA
- If a state law is more restrictive than HIPAA, act as if state law applies
- Key points:
  - Understand timing for required notices; state law requirements often differ from HIPAA
  - State regulators may require notification for ERISA plans
  - Required state law content for notice may differ from HIPAA
  - Both the plan and vendor may be subject to separate notification requirements depending on their roles with respect to the regulated data

McDermott Will & Emery

What are the Security Threats to Benefit Plans?

Examples of Breaches Involving Retirement Plans*

McDermott Will & Emery

- Hacking into the plan's administrative system
- Unauthorized person logging into broker website
- Email hoax (phishing attack) that directed participants to a look-alike website
- Employee downloading confidential information for more than 450,000 participants to a home computer
- PII fraudulently obtained from laptops

*Source: American Institute of Certified Public Accountants.

Examples of Breaches Involving Retirement Plans*

McDermott Will & Emery

- SSNs on documents mailed to wrong addresses or the information was made visible to others
- Employee stealing electronic tapes that contained PII of plan participants and/or beneficiaries
- Auditors who received CDs with PII of participants and beneficiaries in benefit plans they did not currently audit
- Payroll provider using the same password for all clients when the payroll system was established

*Source: American Institute of Certified Public Accountants

Examples of Breaches Involving Welfare Plans*

McDermott Will & Emery

- Breach resulting from unsecured ePHI – unencrypted information on laptops
- Failure to implement physical safeguards at workstations resulting in unauthorized disclosure of ePHI
- Return of multiple photocopiers to a leasing agent without erasing data contained on copier's hard drives
- Lost documents with PHI
- Disposal of prescriptions containing PHI in trash containers accessible to the public

*Source: US Department of Health & Human Services – Phase I Audits

Points of Vulnerability – 2011 ERISA Advisory Council Report

McDermott Will & Emery

- Data management
  - Keeping unnecessary data or data that is no longer relevant
  - No controls over copies and people having access to the data
- Technology management
  - Outdated or poor technology design
  - Inadequate control over wireless and portable devices
  - Failure to use, or improper use of, encryption
- Service provider management
- People issues

Special Concerns with Vulnerability of Protected Health Information (PHI)

McDermott Will & Emery

- FBI Cyber Division – Private Industry Notification (4/8/2014)
  - "[C]yber actors will likely increase cyber intrusions against health care systems. . . due to . . . mandatory transition from payer to electronic health records (EHR), lax cyber security standards, and a higher financial payout for medical records in the black market"
  - "The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors"
  - "Cyber criminals are selling the information on the black market at a rate of $50 for partial EHR, compared to $1 for a stolen social security number or credit card number"

PART III

McDermott Will & Emery

What duty does an ERISA fiduciary have to protect PII/PHI? What is the scope of that duty?

ERISA

McDermott Will & Emery

- ERISA does not expressly address whether, and how, ERISA plans should protect PII
  - Electronic administration a relatively recent phenomenon
- HIPAA provides specific requirements for protecting PHI
- DOL statement – "Understanding Your Fiduciary Responsibilities Under A Group Health Plan"
  - "Mak[e] sure that the plan complies with ERISA, which includes COBRA, HIPAA and other group health plan provisions in the law"
- Discretionary selection of a vendor is a fiduciary function

Applying ERISA General Fiduciary Rules – Privacy and Security Concerns

McDermott Will & Emery

- Who is the fiduciary with delegated authority under the plan document with respect to privacy/security?
  - Protecting PII and PHI
  - Remediating security breaches
- Is someone acting as a fiduciary with respect to privacy/security matters? (ERISA Section 3(18))
- What steps should a fiduciary take to monitor compliance with HIPAA?
  - Insurers, business associates (BAs), subcontractors?

Applying ERISA General Fiduciary Rules – Privacy and Security Concerns (cont.)

McDermott Will & Emery

- What actions should a plan fiduciary take in response to a cybersecurity breach – actions include:
  - Demonstrate actions to investigate the security breach, understand the nature and scope of the breach and identify affected individuals
  - Evaluate HIPAA/state law breach notification requirements – will vendor meet plan's obligations?
  - Communicate with participants – help protect against further fraud, customize notifications and avoid unintended representations
  - Review all agreements between the plan and its vendors
    - Are they signed?
    - Does the promised indemnification protection provide sufficient protection?

Applying ERISA General Fiduciary Rules – Privacy and Security Concerns (cont.)

McDermott Will & Emery

- What information is provided by the plan to participants about actions they can regularly take to protect PII and PHI?
- What reasonable steps can be taken by a plan to protect against elder abuse related to benefit plans?
- Can plan assets be used to cover reasonable security/privacy costs?
- What coverages may be available – fidelity bond for plan? E&O, D&O, ERISA coverage for fiduciaries?

Applying ERISA General Fiduciary Rules – Privacy and Security Concerns (cont.)

McDermott Will & Emery

- Does the plan allow use of its information by vendors, and for what purpose?
  - All Payor Claim Database (APCD) statutes
  - Disclosure to third parties for market research
- Does the plan allow authorized vendors to subcontract to downstream vendors; and if so, for what purpose and how will that data be protected?
- To what extent should a fiduciary review vendor encryption practices?
- What standards of care are imposed on vendors? Are they consistent with ERISA? Other laws?

ERISA Preemption

McDermott Will & Emery

- JCEB Q&A 19 to DOL
  - Alleged state law violation due to administrator providing PII to service providers to generate approved participant communications
  - Proposed answer: “State privacy statutes preempted . . . to the extent that such statutes would otherwise apply to plan administration”
  - DOL declined to answer question – need for “specific state statute . . . and how statute relates to an ERISA . . . plan”
- The extent to which ERISA preempts state law privacy and data breach claims is being actively litigated
- Important for plan fiduciaries to evaluate current practices and vendor commitments in light of state privacy laws

ERISA Preemption (cont.)

McDermott Will & Emery

- Limited case law addressing potential of ERISA preemption of state law privacy claims
- *In re GM*, 3 F.3d 980 (6th Cir. 1993)
  - Alleged breach of EAP confidentiality provision, loss of employment
  - Held: right to privacy claim is preempted by ERISA
- *Vaught v. Hartford Life & Accident Ins. Co.*, 52 Employee Benefits Cas. (BNA) 2659 (USDC S. Dist. of Ohio, 2011)
  - Alleged invasion of privacy due to LTD claim investigation
  - Held: privacy claim not preempted; conduct arguably beyond the bounds of a reasonable investigation

ERISA Preemption
In Re Anthem Data Breach Litigation

McDermott Will & Emery

- Plaintiffs brought case in New York state court asserting various causes of action under New York law, including
  - Negligence, negligence per se, breach of implied contract and covenant of good faith and fair dealing, unjust enrichment and violation of New York's data breach statute
- Defendants removed case to NY federal district court
- Plaintiffs sought to have case remanded to NY state court
- Anthem data breach cases transferred to Judge Lucy Koh in CA federal district court under MDL transfer order
- Judge Koh denies motion to remand (11/24/2015)

ERISA Preemption
In Re Anthem Data Breach Litigation (cont.)

McDermott Will & Emery

- Removal available if federal court would have had subject matter jurisdiction over the case due to a federal question
- Federal question jurisdiction can exist due to ERISA "complete preemption"
- Complete preemption requires that:
  - An individual could have brought a claim for plan benefits under ERISA § 502(a), and
  - there is no other "independent legal duty" that is implicated by a defendant's actions.

ERISA Preemption
In Re Anthem Data Breach Litigation (cont.)

McDermott Will & Emery

- Cause of action was available under §502 to enforce plan rights using breach of contract and unjust enrichment claims
- Plaintiff alleged that ERISA benefits did not include "privacy rights"
- Judge Koh finds to the contrary based on provisions in benefits handbook about compliance with privacy statutes
- State law duties not "independent" of ERISA because benefit plan provisions were as an "essential part" of the claims
- Compare to Rose vs. HealthComp, Inc. (8/10/2015)

ERISA Preemption
In Re Anthem Data Breach Litigation (cont.)

McDermott Will & Emery

- Claims filed in another class action suit alleging violation of NY consumer protection laws that prohibit deceptive acts
- Defendants seek to dismiss claims based on express preemption under §514(a) and conflict preemption
- Key issues:
  - Were promises to protect PII a plan benefit, as defined by ERISA
  - Do state laws that implicate data security "relate to" or conflict with ERISA?
- Judge Koh, citing JCEB Q&A 19, denied motion to dismiss without prejudice due to insufficient information (2/14/2016)

ERISA Preemption
Liberty Mutual v. Gobeille

McDermott Will & Emery

- Vermont imposes All Payor Claim Database reporting obligation
  - APCD statutes compel detailed information about claims and plan members
- Reporting obligation extended to ERISA medical plans
- Plan sponsor refused to authorize TPA to turn over data to Vermont regulators
- Declaratory judgment action filed claiming that ERISA preempted APCD reporting

ERISA Preemption
Liberty Mutual v. Gobeille (cont.)

McDermott Will & Emery

- Supreme Court finds APCD statute preempted under Section 514(a) of ERISA
- ERISA is designed "to provide a single uniform national scheme to administer" plans "without interference" from state law
- Vermont's reporting regime intrudes upon "a central matter of plan administration" and "interferes with nationally uniform plan administration"

ERISA Preemption
Liberty Mutual v. Gobeille (cont.)

McDermott Will & Emery

- State cannot impose supplemental reporting obligation on ERISA plans
- Purpose of supplemental reporting and level of economic burden to plan is irrelevant to preemption analysis
- Decision protects "core" ERISA functions
  - "Reporting, disclosure, and recordkeeping are central to, and an essential part of, the uniform system of plan administration contemplated by ERISA"

ERISA Preemption
Liberty Mutual v. Gobeille (cont.)

McDermott Will & Emery

- Concurring Opinions
  - Thomas questions the constitutional reach of the ERISA preemption provision under the Commerce Clause
  - Justice Breyer suggests that the DOL has authority to issue regulations requiring reporting or perhaps delegating such authority to the states
- Will the DOL work with the states to impose new federal reporting requirements?
  - For medical plans?
  - For retirement plan?

Importance of Vendor Management

McDermott Will & Emery

- Plan fiduciaries responsible for vendor selection and monitoring
- Doing nothing to address privacy and security concerns in the current environment is inconsistent with ERISA fiduciary standards
- Plan fiduciaries and vendors do not always have the same interests
- Actions to comply with state privacy laws may vary
- It is important to protect plan fiduciary's brand and reputation

McDermott Will & Emery

What process can a fiduciary undertake to protect the privacy and security of plan information?

Five Steps Toward Effective Data-Related Vendor Management

McDermott Will & Emery

1. Articulate objectives for data-related vendor management
2. Train stakeholders who work with vendors
3. Establish risk-based, quick-wins approach and process
4. Devise tools for effective data management (e.g., privacy and security contract provisions, due diligence questionnaires, security report requirements)
5. Conduct vendor assessments, ongoing audits of privacy/data security compliance

McDermott Will & Emery

What provisions are appropriate for vendor contracts to protect the privacy and security of plan information?

Bad Example 1: Vendor To Comply With Applicable Privacy Laws

McDermott Will & Emery

Administrative Services Agreement – Vendor to provide certain administrative, accounting and recordkeeping services to the Plan

Provision: Confidentiality

During the term of this Agreement, Service Provider agrees to comply with all international, federal, state, provincial, and local laws, rules, regulations, directives, and governmental requirements currently in effect and as they become effective relating to the privacy, confidentiality, or security of Participant Data, as and to the extent applicable to Service Provider in connection with its obligations under this Agreement (collectively, "Privacy Laws")

Answer: Bad Example 1 – What's Wrong With This Provision?

McDermott Will & Emery

- Privacy laws, in large part, do not apply directly to the vendor
- The plan is likely to be a person that must comply with state privacy laws, not the vendor
- Little-to-no compliance protection for the plan
- Vendor gives "sleeves from its vest"
- Need other data protection provisions that impose compliance obligations on the vendor

Bad Example 2: Vendor Agrees to Treat Personal Information as Confidential Information

McDermott Will & Emery

Master Services Agreement – Vendor required access to all of company's HR personal information for service delivery purposes

Provision: Confidentiality and Data Protection

We will treat as confidential all information (including Personal Information) which you provide to us for the purposes of this Agreement….We confirm that we will only process the Personal Information for the purposes of providing services to you or for other reasonable purposes which are ancillary to the provision of such services

Answer: Bad Example 2 – What's Wrong With This Provision?

McDermott Will & Emery

- Some contracts only contain a confidentiality clause to protect data
- Fails to assist Plan with meeting regulatory obligations for data protection
- Confidentiality is not data security
- Improper disclosures of regulated personal information create different liabilities than improper disclosures of business confidential information

Bad Example 3: Vendor Agrees To Implement Appropriate Security Measures

McDermott Will & Emery

Data Processing Agreement For Cloud Services – Cloud service provider will host company's HR data

Provision: Technical and Organizational Measures

When processing Personal Data on behalf of Customer in connection with the Services, Cloud Provider shall ensure that it implements and maintains compliance with appropriate technical and organizational security measures for the processing of such data

Answer: Bad Example 3 – What's Wrong With This Provision?

McDermott Will & Emery

- Provision is an inadequate legal standard for data security
- Data security regulated by Federal Trade Commission, state laws, EU Data Protection Directive and more
- Lacks specific security measures required to protect the specific personal information made accessible to provider
- Prudent to include a detailed security requirements exhibit as part of a vendor's obligations

Bad Example 4: Return or Destroy Upon Termination or Expiration

McDermott Will & Emery

Administrative Services Agreement – Service provider agreed to provide certain recordkeeping and other administrative services with respect to certain Plans

Provision: Effects of Termination or Expiration

Record keeper agrees that it shall return or destroy all copies (including electronic copies) of Confidential Information (including PII) upon request of the Plan

Answer: Bad Example 4 – What's Wrong With This Provision?

McDermott Will & Emery

- Disposal/destruction of PII subject to state law requirements
- Provision fails to meet typical compliance standard for state law data disposal and destruction of PII
- Regulated PII is held to a higher standard than confidential information for data disposal/destruction
  - Indecipherable, unreadable and unable to be reconstructed

Bad Example 5: Risk Allocation and Indemnity – A Brief Word

McDermott Will & Emery

- Wouldn't we be indemnified if the service provider caused a data breach?
  - It depends
  - If privacy and data security obligations are not explicit, then not likely
  - Even if there is an effective indemnity, it may be capped by the limitation liability
  - Important issues to identify, manage, negotiate and value

Privacy and Data Security Issues List for Contracting with Service Providers

McDermott Will & Emery

Topic	Comments
Provider Due Diligence	**During selection process and prior to contracting, require provider to answer a detailed questionnaire to assess provider's services and its ability to satisfy Plan's compliance needs**
Personal Information	**Define broadly to ensure that it captures all regulated information that will be accessed by provider – it's not just PHI. Plan is the owner of its information, not the provider**
Privacy Laws	**Define broadly to encompass U.S. state and federal laws and any other applicable national laws addressing privacy and security obligations and any applicable industry standards (i.e., Payment Card Industry Data Security Standards)**
Compliance with Privacy Laws	**Provider should acknowledge that the services require the processing of the plan's personal information and that it will comply with the privacy laws that govern that personal information**
Roles	**Clarify that provider shall only act according to a named fiduciary's instructions**

Privacy and Data Security Issues List for Contracting with Service Providers (cont.)

McDermott Will & Emery

Topic	Comments
Cooperation	**Provider should agree to provide information and support as the plan may require to comply with privacy laws**
Confidentiality	**Provider must agree to keep the personal information confidential according to the confidentiality clause. It is important to ensure that the typical confidentiality exclusions do not apply to personal information**
Restricted Use	**Provider must agree to limit its use of the personal information to the delivery of services specified in contract and for no other purpose**
Privacy	**Obligate the provider to comply with privacy laws applicable to the plan's personal information**
Security	**Provider must agree to provide security according to 2 standards: (1) security as crafted from data security laws applicable to the plan's personal information; *and* (2) as specified for the particular services. Involve IT Security to assess level of security offered by provider. Tie obligations to an industry security standard, i.e., ISO 27001**

Privacy and Data Security Issues List for Contracting with Service Providers (cont.)

McDermott Will & Emery

Topic	Comments
Data Security Breach	**Define broadly to include suspected breaches and establish procedures in the event of a breach. Require provider to notify, investigate, remediate, assist the plan with any required notices to affected individuals and as required to determine the extent of the breach and to contact affected individuals**
Reimbursement	**Provider should be required to reimburse plan for costs, expenses and other damages incurred by the plan due to the data security breach**
Audit Rights	**Plan should have the right to monitor the provider's performance as it is required by many privacy laws. Provider should be obligated to provide audit reports that apply to the services (i.e., AICPA's SOC 2 Report) and ensure that such reports cover the appropriate timeframe**
Data Transfers	**Plan should specify that personal information can only be processed and stored in the U.S. if that is the case. Location should be specified and, if outside of the U.S., data could be subject to legal requirements of other jurisdiction. If EU data is transferred outside of the EU, issues dealing with data transfer restrictions need to be addressed (i.e., Safe Harbor, Model Contractual Clauses)**

Privacy and Data Security Issues List for Contracting with Service Providers (cont.)

McDermott Will & Emery

Topic	Comments
Risk Allocation – Indemnity/Limitation of Liability	**Highly negotiated. Not regulated but reflects benefit of bargain. Seek to have provider reimburse Plan for expenses, costs, and other damages associated with a data breach occurring under vendor's control. Best case: Provider provides unlimited hold harmless indemnity for all claims resulting from its breach of confidentiality, privacy and security provisions. Worst case: An indemnity limited by a cap in the limitation of liability that's' too low to provide plan sufficient protection**
Disposal and Deletion	**Provider must return or destroy at end of agreement. If data to be destroyed, provider must be obligated to destroy consistent with state privacy laws (i.e., shredded, erased, or otherwise modified such that the personal information is unreadable or undecipherable through any means)**
Privacy Contact	**Provider should designate a privacy contact point person to handle inquiries from the plan about the data**