Life Sciences 2022: At Home & Across the Globe

Virtual CLE & Live Networking Event, May 11-13, 2022

ReedSmith

Driving progress
through partnership

Speakers

Sarah Bruno
Partner-Reed Smith
San Francisco
+1 415 659 4842
sbruno@reedsmith.com

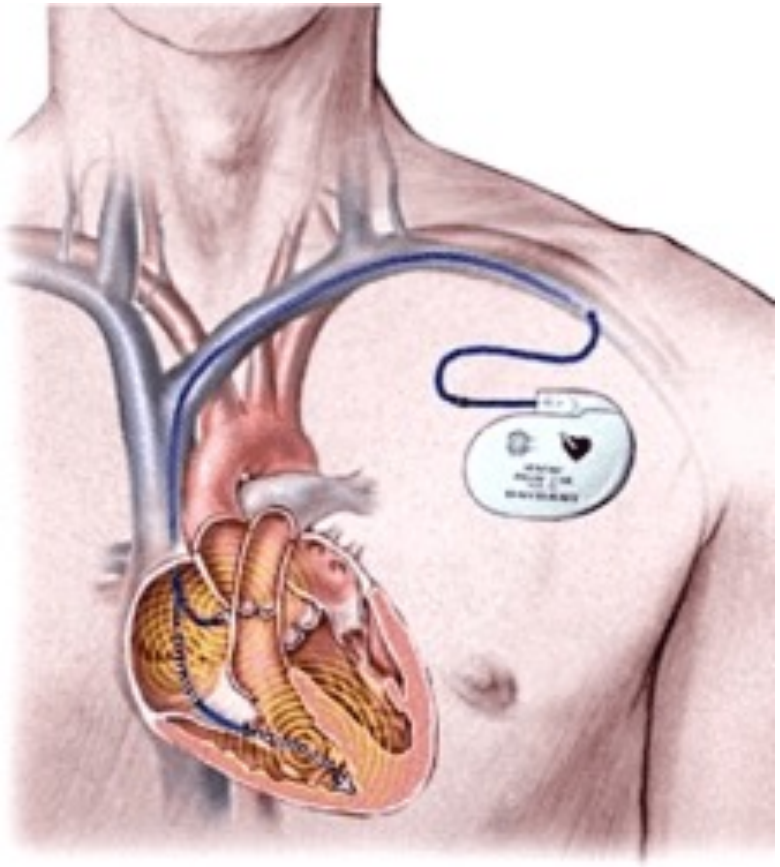
Catherine David
Associate-Reed Smith
Philadelphia
+1 215 241 7913
cdavid@reedsmith.com

Daniel Marcus-Toll
Senior Counsel-Gilead
New York
+1 650 398 2608
daniel.marcustoll@gilead.com

Agenda

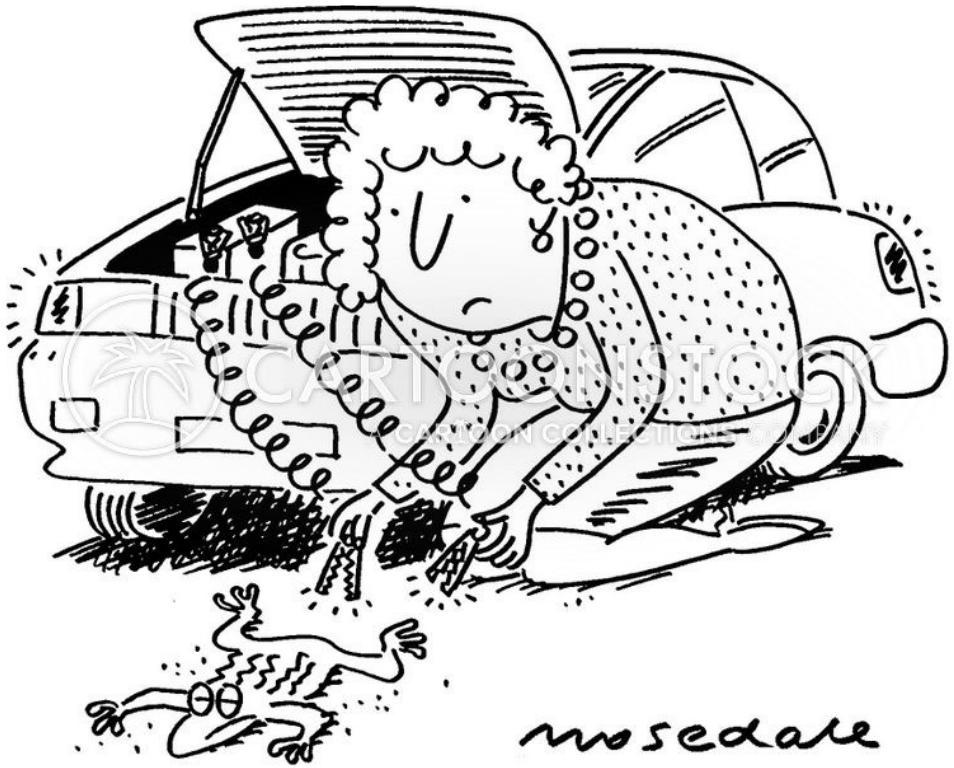
- Hypothetical
- Nature of Data Collected
- Data Collections
- Jurisdictions & Compliance Obligations
- Distribution Model
- Marketing Considerations

Hypothetical



Nature of Data Collected & Collection Methods

Jump Starter – Medical Device



Types of Data Collected Once Implanted:

- Name
- Address
- Contact information
- Health care provider information
- Medical device ID
- Health information

Method of Collection: Implanted device that transmits data

Heart Boost – Pharmaceutical

Types of Data Collected Pre-Market:

- Clinical Trial Data (previous and ongoing medical history); name, address, contact information

Method of Collection:

- Direct from patient, or from Covered Entity via HIPAA Authorization, IRB Waiver of HIPAA Authorization, or use of Limited Data Set.

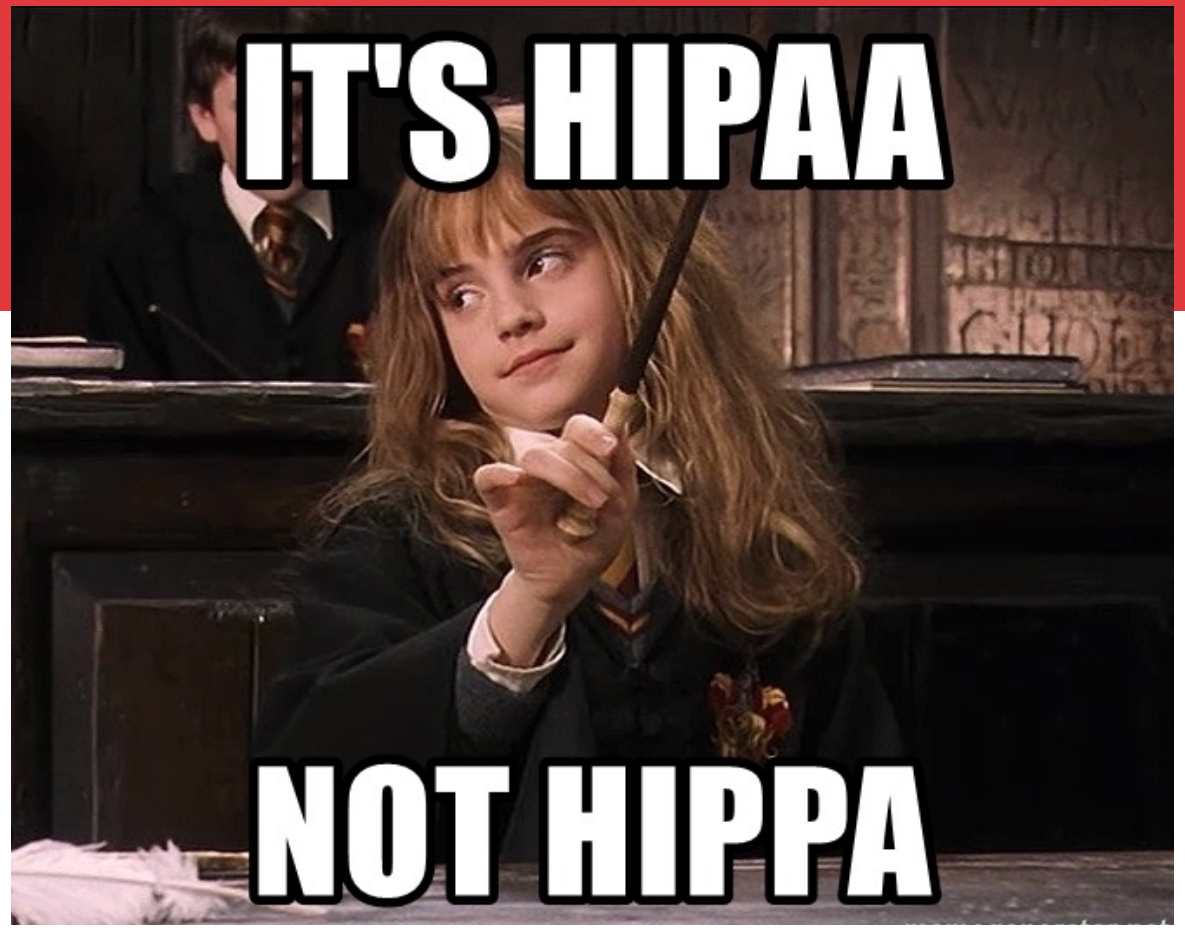
Jurisdictions & Compliance Obligations

Jurisdictions

HIPAA & State Law

GDPR

HIPAA



Our Favorite HIPAA Misconception

~~HIPAA applies to all health information~~

HIPAA-Applies To…

Health Plans: employer group health plans, health insurance carriers, etc.

Health Care Clearinghouses: processes/facilitates processing information from a nonstandard format to a standard format

Health care providers: physicians, clinics, hospitals, provided they engage in an *electronic covered transaction*

Business Associates: A person or entity that performs certain functions or activities for or on behalf of a covered entity that require the person or entity to create, receive, maintain or transmit PHI.

Examples include:

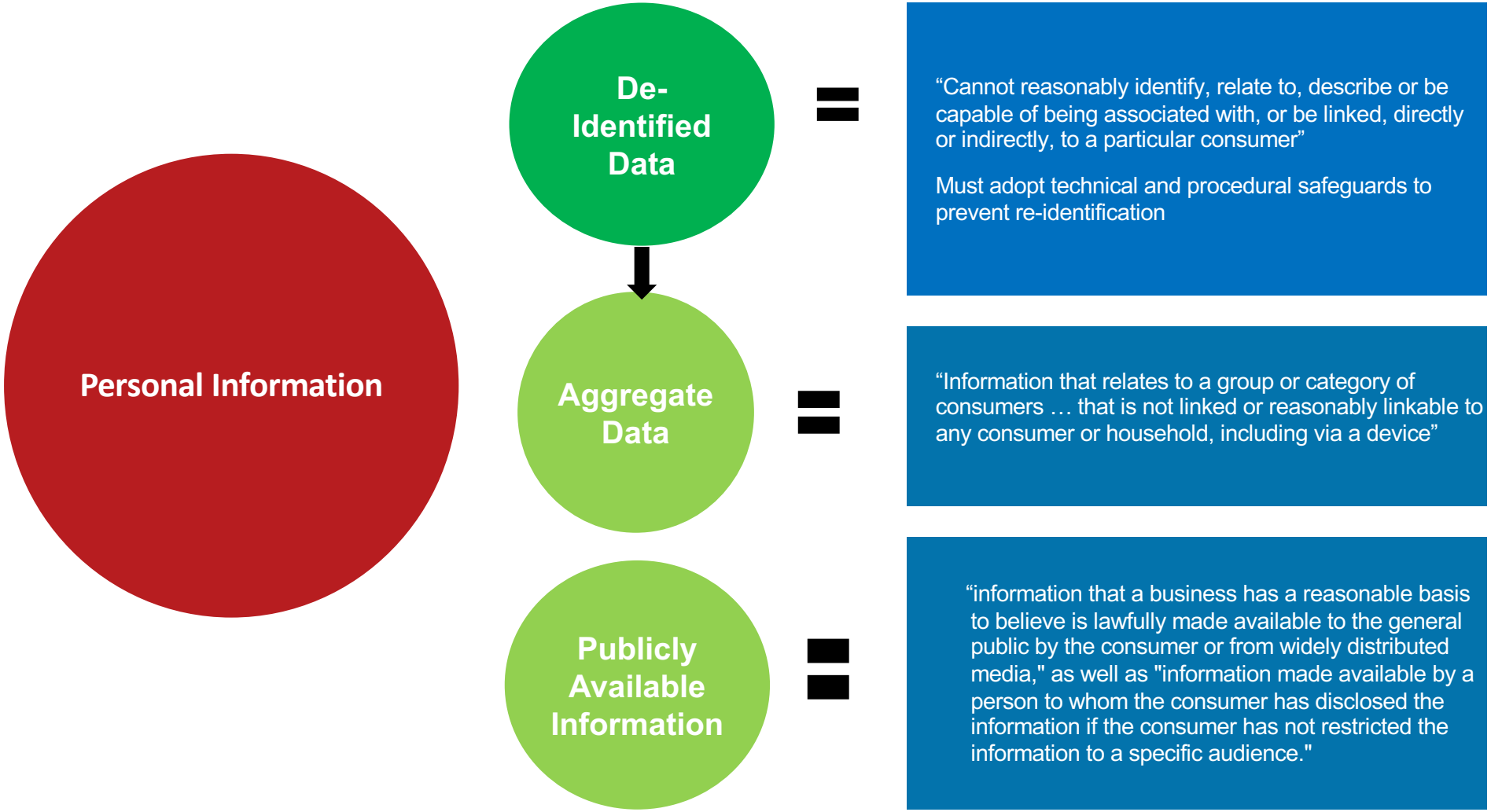
- Electronic medical records vendor
- Patient portal vendor
- Call center
- Printer/copier/eFax companies
- Lawyers, accountants, consultants

Regulation of Medical Device & Pharmaceutical Manufacturers

How to conduct clinical research with ‘HIPAA’ Data

1. Patient authorization
2. IRB waiver of the authorization requirement
3. De-identified data
4. Limited data

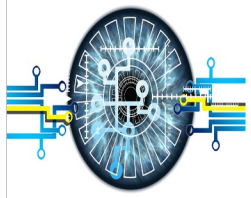
State & International Data Privacy Laws


Personal Information
De-Identified Data
=
"Cannot reasonably identify, relate to, describe or be capable of being associated with, or be linked, directly or indirectly, to a particular consumer"
Must adopt technical and procedural safeguards to prevent re-identification
Aggregate Data
=
"Information that relates to a group or category of consumers … that is not linked or reasonably linkable to any consumer or household, including via a device"
Publicly Available Information
=
"information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media," as well as "information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience."

CPRA

“Sensitive Personal Information” is information that reveals:

- **SSN or government IDs**
- **Details about a consumer’s financial information or accounts**
- **Precise geolocation information**
- **Information about race, ethnicity, religion, or philosophical beliefs**
- **The contents of a consumer’s communications**
- **Genetic data**
- **Processing of biometric information for the purpose of uniquely identifying a consumer**
- **Personal information collected and analyzed concerning a consumer’s health or sex life/sexual orientation**



CMIA

Regulated Actors: Health care providers, health care service plans, pharmaceutical company and contractors

Regulated Information: Individually identifiable information, in electronic or physical form regarding a patient's medical history, mental or physical condition, or treatment

Limitations on Use and Disclosure

Illinois: Biometric Information Privacy Act

- Regulates “biometric information” and “biometric identifiers”
- **“Biometric information”** means any **information**, “regardless of how it is captured, converted, stored, or shared,” **based on an individual’s biometric identifier used to identify an individual**. Biometric information does not include information derived from items or procedures excluded under the definition of “biometric identifier.”
- **“Biometric identifier”** means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. The law expressly excludes certain data elements from the definition of “biometric identifier” (e.g., writing samples, photographs, tattoo descriptions, information captured in a healthcare setting or under HIPAA, etc.).

GDPR

- **The GDPR regulates "Data Concerning Health"**
  - Data Concerning Health is information relating to a natural person's past, current, or future physical or mental health that reveals information about that person's health status.
  - Data about health is considered special category data under GDPR Article 9
  - Examples of Health Data enumerated in Recital 35 include:
    - Information about the natural person collected in the course of registration of or the provision of health care services;
    - A number, symbol, or particular assigned to a natural person to uniquely identify the person for health purposes;
    - Information derived from he testing or examination of a body part or bodily substance, including genetic data and biological samples;
    - And any information on a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent from its source (e.g. from a physician).

Informed Consent

Informed consent means the data subject knows your identity, what data processing activities you intend to conduct, the purpose of the data processing, and that they can withdraw their consent at any time.

Distribution Model-Vendor Contracts

Know your Vendors

1. **Expertise & Duration of Service**
2. **Jurisdictions involved**
   - **Place of Business**
   - **Data Storage**
   - **Employees with Access**
3. **Security Considerations**

Jurisdictional Considerations

Processor/Controller Obligations

- **Data Minimization & Purpose Limitation**
- **Reasonable Data Security**
- **Consent for Processing of Sensitive Data**
- **Privacy Notice**
  - Must disclose categories and purpose of PI collected, how to exercise rights, categories of data shared, and categories of third parties data shared with
- **Disclosure of Sale of Data or Targeted Advertising**
- **Controller—Processor Contract Required**
- **Data Protection Impact Assessments**

Transfer Considerations

- **Cross-border transfers of personal information, including health data, must be carried out in compliance with Articles 45-47 of the GDPR.**
  - Generally speaking, health data may lawfully be transferred only if one of the following requirements is met:
    - There is an EU Commission Adequacy Decision that covers the recipient country;
    - Both the data exporter and importer have adopted Binding Corporate Rules ("BCR"); or
    - EU Model Standard Contractual Clauses ("SCCs"), governing the security of the data transfer, have been executed by the exporter and importer parties.
- **On March 25, 2022, the European Commission and the United States reached an agreement in principle for a Trans-Atlantic Data Privacy Framework.**
  - Based on the new framework, data will be able to flow freely between the EU and U.S. Companies
  - A new set of rules and binding safeguards t limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security;
  - The framework establishes a new two-tier redress system to investigate and resolve complaints of EU residents on the access of data by U.S. Intelligence authorities, which includes a Data Protection Review Court.
  - Additionally, the framework creates obligations for companies processing data transferred from the EU, which will require entities to self-certify their adherence to the Principles established in the Framework through the U.S. Department of Commerce.

US - DPA Considerations - CA

CCPA:

Written contract must:

(i) Prohibits Service Provider receiving the personal information from:

(a) Selling the personal information.

(b) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(c) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Include a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

US – DPA Considerations - CA

CPRA General Contractual Requirements:

A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:

- Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes.
- Obligates the third party, service provider, or contractor to comply with applicable obligations under the CPRA and obligate those persons to provide the same level of privacy protection as is required by the CPRA.
- Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under the CPRA.
- Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under the CPRA.
- Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

US – DPA Considerations - CA

CPRA - Contractors

What is a contractor?

- A “contractor” is a person to whom the business “makes available” a consumer’s personal information for a business purpose.
- “Contractors” are distinguishable from “service providers” that “process personal information on behalf of a business.”
- A “contractor” may be a more appropriate designation for an organization that receives personal information as part of providing a service to the disclosing organization (rather than receiving the information for its own commercial purposes) but is still **not processing personal information solely on behalf of the business** and/or that exercises autonomy over its use of personal information

US – DPA Considerations

What is a contractor?

- A “contractor” is a person to whom the business “makes available” a consumer’s personal information for a business purpose.
- “Contractors” are distinguishable from “service providers” that “process personal information on behalf of a business.”
- A “contractor” may be a more appropriate designation for an organization that receives personal information as part of providing a service to the disclosing organization (rather than receiving the information for its own commercial purposes) but is still **not processing personal information solely on behalf of the business** and/or that exercises autonomy over its use of personal information

US – DPA Considerations – VA/CO

Contract Must Include:

- Instructions for processing
- Nature and purpose of processing
- Type of data subject to processing
- Duration of processing
- Rights and obligations of both parties

Processor must:

- Duty of confidentiality
- Delete or return data at the end
- Establish compliance
- Assessments
- Subcontractors must meet these obligations

CCPA Requirements

Written contract must:

(i) Prohibits Service Provider receiving the personal information from:

(a) Selling the personal information.

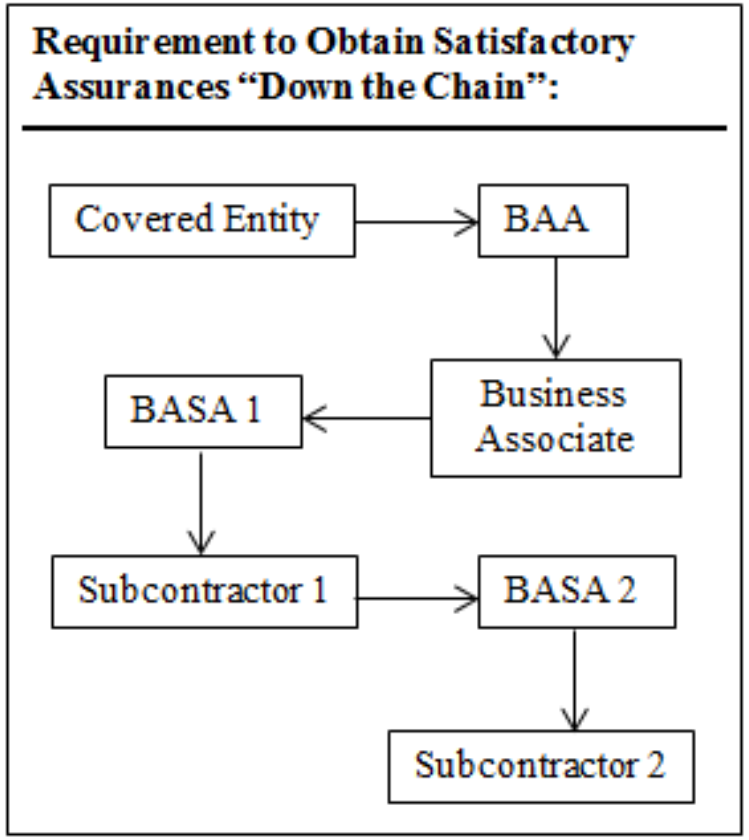
(b) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(c) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Include a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

HIPAA-Business Associate Agreement

- Covered entities must contractually bind business associates through BAAs
- Business associates must then contractually bind their subcontractors to these same rules (through business associate subcontractor agreements or BASAs)
- Evaluate arrangements where a third party creates, receives, maintains, or transmits PHI on behalf of your organization
- HIPAA requires that certain terms be included in BAAs, outlined at 45 CFR § 164.504(e) – review each BAA to confirm compliance.
- Ensure appropriate designation of parties



Marketing Considerations

CAN-SPAM Act

Background

In effect since January 1, 2004

Sets forth a series of requirements and prohibitions relating to "commercial" and "transactional or relationship" email messages

(1) Accurate email transmission information,

(2) Identification of the email sender's physical location, and

(3) Provision of an opportunity to opt out of receiving future mailings.

Who Can Enforce the CAN-SPAM Act?

Federal agencies, including the FTC and the Department of Justice, certain state law enforcement authorities, and Internet service providers, may file civil suits to halt unlawful spammers.

Primary Requirements

1. **Don’t use false or misleading header information.** Your “From,” “To,” “Reply-To,” and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
2. **Don’t use deceptive subject lines.** The subject line must accurately reflect the content of the message.
3. **Identify the message as an ad.**
4. **Tell recipients where you’re located** (e.g., include a valid physical postal address).

Primary Requirements

5. **Tell recipients how to opt out of receiving future email from you** (e.g., a return email address). Notice must be easy for an ordinary person to recognize, read, and understand. Make sure your spam filter doesn't block these opt-out requests.

6. **Honor opt-out requests promptly.** Within at least 10 business days.

- You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, etc..
- After removal, you can't sell or transfer their email addresses, even in the form of a mailing list.

7. **Monitor what others are doing on your behalf.** Even if you hire another company to handle your email marketing.

Telephone Consumer Protection Act (TCPA)

Purpose

- Law restricts telemarketing certain phone calls, text messages, and facsimiles
- Rules apply to common carriers as well as to other marketers.

Primary Requirements

Telemarketers must:

(1) obtain prior express written consent from consumers before robocalling them,

(2) no longer use an "established business relationship" to avoid getting consent from consumers when their home phones, and

(3) provide an automated, interactive "opt-out" mechanism during each robocall so consumers can immediately tell the telemarketer to stop calling.

Who May Assert a Claim Under TCPA?

- Consumers may file complaints with Federal Communications Commission (FCC) when TCPA is violated.
- Since TCPA law governs consumer rights, lawsuits may also be filed by consumers who suffer violations.

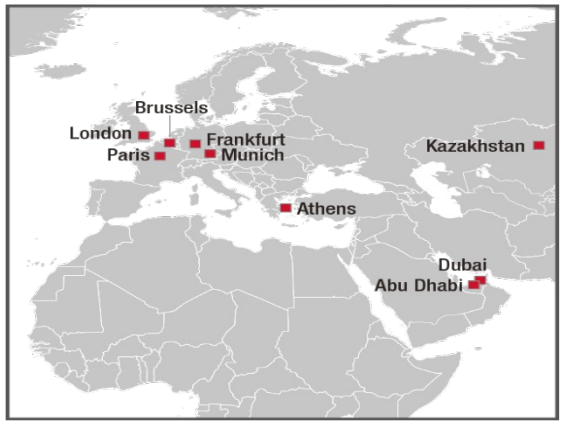
Questions?

ABU DHABI
ATHENS
AUSTIN
BEIJING
BRUSSELS
CENTURY CITY
CHICAGO
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward.

Reed Smith is a dynamic international law firm dedicated to helping clients move their businesses forward. With an inclusive culture and innovative mindset, we deliver smarter, more creative legal services that drive better outcomes for our clients. Our deep industry knowledge, long-standing relationships and collaborative structure make us the go-to partner for complex disputes, transactions, and regulatory matters.

For further information, please visit reedsmith.com



reedsmith.com

ReedSmith
Driving progress
through partnership