Overview of Privacy Requirements and Compliance Issues in International Clinical Trials

Health Care Compliance Association
Research Compliance Conference
October 18-20, 2009
Minneapolis, MN

Today’s Presenters

◆ Paul R. DeMuro, J.D., CHC, CPA, MBA
  □ Partner
  Latham & Watkins LLP
  San Francisco, CA and Los Angeles, CA

◆ John E. Steiner, Jr., J.D., CHC, CCEP
  □ Chief Compliance Officer
  University of Kentucky HealthCare,
  Lexington, KY
Overview of Privacy Requirements and Compliance Issues

- Confidential patient information may be used improperly or even criminally by an unauthorized recipient
- Market has not self-regulated; thus, increase in state, federal and international information privacy laws and regulations
- Privacy laws affect pharmaceutical companies and other healthcare research organizations involved in international clinical trials
- Key Questions: How is personal information stored, transmitted, used and disclosed?

Overview

- Some international laws prohibit companies located in countries that lack adequate privacy protections from importing personal information unless additional steps are taken
- International clinical trials subject to the jurisdiction of the U.S. Food and Drug Administration have increased substantially over the past 15 years.
The FDA issued new regulations on April 28, 2008, revising the standards for acceptance of data from foreign non-Investigational New Drug (IND) clinical trials to support domestic applications and submissions. (21 C.F.R. 312.120)

- The FDA has become more cautious in relying on data collected from foreign studies due to the difficulty in verifying the data.

Overview

- Trials cross borders because:
  - High quality trials are conducted in other countries
  - Potential mitigation of liability
  - Availability of an understandable and harmonized legal framework
Overview

- Movement toward harmonizing standard rules for governing clinical trials: International Conference on Harmonization (ICH) of Technical Requirements for Regulation of Human Use
- Clinical practice guidelines and standards that are accepted by the FDA and European regulatory authorities
- ICH Harmonized Triparte Guidelines- Guidelines for Good Clinical Practice (GCP)

GCPs Defined

- GCPs are generally accepted, international best practices for conducting clinical trials and device studies
- They are defined as an international ethical and scientific standard for designing, conducting, recording and reporting trials that involve the participation of human subjects
- They are NOT statutes or regulations and do not have the force of law
  - Compliance with GCPs provide public assurance that the rights and safety of participants in human subject research are protected and that the data that arises from the study is credible
The Core of the Consolidated GCP Guidance

The thirteen principles of GCP are the key to assuring the acceptance of clinical trial data among the nations involved.

<table>
<thead>
<tr>
<th>The Thirteen Principles of GCP Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Clinical trials should be conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki, and that are consistent with GCP and the applicable regulatory requirements</td>
</tr>
<tr>
<td>2. Before a trial is initiated, foreseeable risks and inconveniences should be weighed against the anticipated benefit for the individual trial subject and society. A trial should be initiated and continued only if the anticipated benefits justify the risks</td>
</tr>
<tr>
<td>3. The rights, safety, and well-being of the trial subjects are the most important considerations and should prevail over interests of science and society</td>
</tr>
<tr>
<td>4. The available non-clinical and clinical information on an investigational product should be adequate to support the proposed clinical trial</td>
</tr>
<tr>
<td>5. Clinical trials should be scientifically sound, and described in a clear, detailed protocol</td>
</tr>
<tr>
<td>6. A trial should be conducted in compliance with the protocol that has received prior institutional review board (IRB)/independent ethics committee (IEC) approval/favorable opinion</td>
</tr>
<tr>
<td>7. The medical care given to, and medical decisions made on behalf of, subjects should always be the responsibility of a qualified physician or, when appropriate, of a qualified dentist</td>
</tr>
<tr>
<td>8. Each individual involved in conducting a trial should be qualified by education, training, and experience to perform his or her respective tasks</td>
</tr>
<tr>
<td>9. Freely given informed consent should be obtained from every subject prior to clinical trial participation</td>
</tr>
<tr>
<td>10. All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation, and verification</td>
</tr>
<tr>
<td>11. The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirements</td>
</tr>
<tr>
<td>12. Investigational products should be manufactured, handled, and stored in accordance with applicable good manufacturing practice (GMP). They should be used in accordance with the approved protocol</td>
</tr>
<tr>
<td>13. Systems with procedures that assure the quality of every aspect of the trial should be implemented</td>
</tr>
</tbody>
</table>
The ICH Guideline for GCP is specific about data collection, data handling, documentation and retention of records (see: ICH GCP §5.12, 5.15 and 6.10)

The basic purpose of ICH GCP is to promote best practices in clinical trials, not necessarily to provide privacy guidelines.

The ICP GCP does contain standards on record access and patient subject consent, audit procedures, and sponsor access to source data (e.g. medical records)

Under ICH GCP, investigators must provide sponsors, monitors, and regulatory agencies with direct access to “source date/documents” for purposes of monitoring, auditing, IRB review, and regulatory inspections.

(See: ICH GCP §1.51, 1.52, 5.1.2, 5.15.1 and 6.10)
Privacy and Data Protection Global Perspective

Risk Assessment Steps:

- Within the organization, who is responsible for privacy
- How is the Privacy Program structured?
- How are Policies & Procedures implemented and integrated with current compliance activities

Do Departments work together to ensure that privacy practices are uniform

What third parties have access to the organization’s information system

What type of personal information is used and disclosed by the organization

Who receives personal information from the organization
■ What are future plans and proposed budgets to improve compliance within the organization
■ How to optimize change management methods to implement a comprehensive privacy and security compliance program

Data Protection Global Legal Matrix

Variables by Country (Area) and Law:

<table>
<thead>
<tr>
<th>Country</th>
<th>Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>HIPAA</td>
</tr>
<tr>
<td>European Union</td>
<td>EU Data Protection Directive</td>
</tr>
<tr>
<td>Canada</td>
<td>Personal Information Protection and Electronic Documents ACT (PIPEDA)</td>
</tr>
<tr>
<td>Japan</td>
<td>Personal Information Protection Act (PIPA)</td>
</tr>
</tbody>
</table>
Variables by Privacy Standards:

- Information Protected
- Entities Covered by Law
- Privacy Official
- Enforcement Authority
- Staff Training Required
- Data Owner
- Data Recipient
- Database Registration
- Etc. (See: Resource matrix at end of slides)

As the Western European countries have no considerable cost or patient enrollment advantages with respect to the United States, over the past decade or so pharmaceutical companies have been attracted increasingly to the countries of Central and Eastern Europe (CEE). The advantages to placing clinical trials in this area are:
The countries beyond the scope of the EU Clinical Trials Directive follow their own individual legal regimes.

The CEE countries whose legislation and administration regarding clinical trials are modeled according to the EU Clinical Trial Directive are: Estonia, Latvia, Lithuania, Poland, Czech Republic, Slovakia, Hungary, Romania, Bulgaria, and Slovenia.
The CEE countries to which the directive does not apply are: Croatia, Bosnia Herzegovina, Serbia and Montenegro, Macedonia, Albania, Belorussia, Ukraine, Moldova, and Russia.

Directive 2001/20/EC

- Background and scope
- Significant innovations
- Achievements and limitations
Background of the Directive

- Framework required to protect clinical trials subjects
- Absence of harmonization among Member States
- Lack of legal text on the application of GCP and GMP
- Unification of information and pharmacovigilance

Scope of the Directive

- All European Union (EU) Member States are involved in the EU Directive
- All trials except for non-interventional trials
- Broader definition of clinical trials
  - Refers to trials in “human subjects” which includes healthy volunteers
  - Does not differentiate between commercial and non-commercial trials
Significant Innovations of the Directive

- Database on clinical trials (EudraCT)
  - Regulatory overview of clinical trials
  - Exchange of information
- Protection of clinical trial subjects
  - Benefit from the trial
  - Informed consent
  - Specific rules concerning minors and incapacitated adults
  - Data protection measures
  - Insurance

Significant Innovations (cont.)

- Harmonization of the authorization procedure
  - Application review within 60 days
  - Parallel submissions to Ethics Committee (EC) and Competent Authority (CA)
  - “Single opinion” rule for multi-center trials
- Increased responsibilities of the sponsor
  - Quality insurance and quality control
  - Notification/submission to regulatory authorities
  - IMP/GMP compliance
  - Ongoing safety evaluation and adverse event reporting
  - Sponsor may delegate aspects of clinical trials (e.g. to CRO) whilst retaining overall responsibility
Major Achievements and Limitations

- Achievements
  - Free movement of Investigational Medicinal Products (IMPs)
  - Timeline can be monitored
  - Standardization of the documentation
  - Generation of a competitive market for clinical trials in Europe

- Limitations
  - Strengthening the protection of clinical trials subjects
  - IMPs only manufactured at licensed manufacturing sites
  - Inspections to assess compliance with GMP and GCP
  - Establishment of a legal representative for non EU sponsor
  - Lack of centralization
  - Incomplete harmonization

Summary of the EU Clinical Trials Directives

All interventional clinical trials are covered by the EU Clinical Trials Directive and require authorization by each member state’s regulatory body.

Key points of the EU clinical trials directive are:
Protection of clinical trial subjects: The directive pays special attention to the protection of clinical trial subjects and informed consent.

Procedures for ethics committees: The directive defines the procedures for ethics committees, including a time limit for decisions.

Absolute deadlines for the assessment of clinical trial applications: Both the regulatory body and ethics committee have to approve of the clinical trial.

Exchange of information between the regulatory body, the sponsor and the European Agency for the Evaluation of Medicinal Products (EMEA): EMEA hosts a safety and information database on clinical trials, called EudraCT.
Summary of the EU Clinical Trials Directive (con’t)

- Standards for Good Clinical Practices (GCP) and good manufacturing practices (GMP): All manufacturers of investigational medicinal products (IMPs), including placebos and active comparator products, require a manufacturing license. All IMPs must be manufactured according to GMP.

Summary of the EU Clinical Trials Directive (con’t)

- Pharmacovigilance: Unexpected serious adverse events (SAEs), if fatal or life-threatening, are to be reported within seven days of knowledge by sponsor. All other suspected SAEs must be reported within 15 days of first knowledge by the sponsor.
The implementation of the EU Clinical Trials Directive was not universally considered a success according to some reports.

Costs for clinical trials have increased up to 85 percent in certain countries, leading to a decrease in clinical trial activities in a number of EU member states, in particular certain member states belonging to the CEE territory.

On the timeline, a number of newly admitted EU member states belonging to the CEE region have lost their competitive advantage of speedy clinical trial approval. Thus, it is no surprise that Russia and Ukraine, with their substantial populations and not falling under the EU regime, are among the fastest growing clinical research areas of the world.
Summary of the EU Clinical Trials Directive (con’t)

What draws sponsors to those countries are:

- Rapid study initiation (typically 10 to 15 weeks from document submission to enrollment of the first patient);
- Academic centers and specialized hospitals for all therapeutic areas;
- Western medical technique processes; and
- High enrollment rates and drug naïve patients in many therapeutic areas

Key Considerations

- Risk Management
  Close risk management is crucial for the success of clinical trials in these countries
- Equipment and Training
  Equipment is also an important consideration along with study-specific training
Key Considerations

- Standards and Documentation
  Sponsors should make sure that they have a good knowledge of local requirements and timelines to submit documents in accordance with the laws of the various countries.

Comparison of Clinical Trials in the EU and the US

- Regulatory documents submissions
- Protection of clinical trial subjects
- Investigational medical product (IMP) issues
Regulatory Document Submission

**EU**
- Application Submission
  - One CA submission per Member State (MS)
  - 25 countries / 25 authorizations
- Protocol
  - Stand alone submission to CA for each protocol
  - 60 day review timeframe
  - MS can impose shorter timeframe per national law

**US**
- Application Submission
  - One regulatory authority at the federal level – the FDA
  - Single submissions
    - Single authorizations
- Protocol
  - New protocol submitted as amendment to IND of the investigational product
  - 30 day FDA review timeframe
  - No official review timeframe for amendments to the IND

Protection of Clinical Trial Subjects

**EU**
- Minimal detail on ICD
- Minors & incapacitated adults
  - No incentives or financial inducements allowed
- Some countries require insurance info to be put into ICD
- No provisions outlined for emergency consent
- European Commission Directive 95/46

**US**
- Detailed list of ICD requirements
- All subjects
  - Disclosure of anticipated prorated payment, if any, to the subject for participation
- No requirement for insurance info on ICD
- Provisions for emergency consent
- Local sites required to incorporate HIPAA regulations into consent process
Investigational Medicinal Products Issues

EU
- Manufacturing and Import
  - Must be manufactured to a standard "at least equivalent" to EU GMP
  - Import authorization required via application to a CA
  - Once within EU, shipment between MS does not require any further import authorization

US
- Manufacturing and Import
  - Must satisfy US GMP
  - Import of investigational product provided to a consignee as defined in the IND
  - Unrestricted shipment between US states

Investigational Medicinal Products Issues (cont.)

EU
- Labeling
  - Label samples may be required by ECs
  - Must be in the official language(s) of the MS on the outer package, or where not outer package, on the immediate packaging
  - Labels require expiration date

US
- Labeling
  - Label samples not required by IRBs
  - Label must bear specific language ("Caution: new drug limited by...")
  - Labels do not require expiration dates
New Standards For Foreign Clinical Trials

- Foreign clinical trials to be used as support for an IND, new drug approval (NDA), or abbreviated new drug approval (ANDA) application must be conducted pursuant to the oversight of an IEC and in compliance with the FDA’s GCP regulations.

New Standards For Foreign Clinical Trials (cont.)

- The revisions to the regulations for foreign, non-IND clinical trials require sponsors to (1) demonstrate that the studies are conducted in accordance with GCP; and (2) permit the FDA to validate the data through onsite inspection. Compliance with GCP requires, among other things, patient informed consent, investigator statements, and adverse event and periodic reporting to the FDA.
New Standards For Foreign Clinical Trials (cont.)

- The GCP regulations also require that the study be conducted under the oversight of an IEC — “a review panel that is responsible for ensuring the protection of the rights, safety, and well-being of human subjects involved in a clinical investigation and is adequately constituted to provide assurance of that protection.”

New Standards For Foreign Clinical Trials (cont.)

- The GCP standards require IEC review and approval of the study protocol before initiation of a study, continuing IEC review of an ongoing study, and IEC approval for obtaining and documenting informed consent.
The revised regulations describe the information that must be provided when a clinical trial sponsor submits foreign clinical data to the FDA in support of an IND, NDA, or ANDA. These data submission requirements include a description of investigator qualifications, research facilities, drug product, study protocols, and results.

The FDA also has added a record retention requirement, which lasts for two years after the agency’s decision on an application for marketing approval or, if a study is submitted in support of an IND but not an application for marketing approval, for two years after the submission of the IND. The purpose of this record retention requirement is to enable FDA onsite inspection, if necessary.
The new regulations do not grandfather trials in progress. The new requirements for the design, conduct, and reporting of foreign clinical trials will apply equally to studies that result in NDA and ANDA applications for domestic marketing approval.

The Report “The Case for Globalization: Ethical and Business Considerations in Clinical Research,” was conducted for the Washington-based Association of Clinical Research Organizations (ACRO)

The vast majority of such research continues to be conducted in countries with well-established infrastructures.
Clinical trials are being conducted more frequently in emerging countries in order to tap into greater resources of people for use as trial subjects and, as a consequence, to make lifesaving drugs more readily available in these countries.

Clinical Trials abroad are generally subject to the same standards that prevail in the developed world, particularly industry-sponsored trials.

BNA noted that the “Report” notes that:

- Increased demand for clinical trial subjects combined with lower participation rates in developed countries has the potential to dramatically slow the progress of medical science.

- Globalized trials speed drug development.

- Regulatory and cultural norms regarding clinical research in emerging countries often are more, rather than less, strict than in developed regions.
Clinical research plays an important role in improving the health systems and economies of emerging countries.

The term “emerging market” disguises a wide range of experience levels. After 15 years of experience with clinical trials, capabilities of the larger Central European countries are considered to be very nearly on a par with those in Western Europe.

The report is available at:

http://www.acrohealth.org/globalization/
Globalization.pdf
The Food and Drug Administration announced a partnership August 3, 2009 with its European counterpart to ensure that clinical trials submitted in drug marketing applications in the United States and Europe are conducted uniformly, appropriately, and ethically.

The Good Clinical Practices Initiative is an agreement between FDA and the European Medicines Agency (EMEA) that began September 1, 2009. The program focuses on collaborative efforts to inspect clinical trial sites and studies, particularly on products regulated by the FDA Center for Drug Evaluation and Research in the United States and by the EMEA for the European Union.
According to the FDA, BNA reports the GCP initiative has several goals:

- To conduct periodic exchanges of GCP-related information to streamline sharing of GCP inspection planning information and communicate timely and effectively on inspection outcomes.

- To conduct collaborative GCP inspections by sharing information, experience, and inspection procedures, cooperating in the conduct of inspections, and sharing best-practice knowledge; and
To share information on interpretation of GCP by keeping each regulatory agency informed of GCP-related legislation, regulatory guidance, and related documents and to identify and act together to benefit the clinical research process.

At the conclusion of the pilot phase, FDA said the agency will make a joint assessment with EMEA, with the scope and process modified, and amended as needed.

More information on the FDA-EMEA agreement is available at:

**Additional Resource link:**

http://www.privireal.org/

<table>
<thead>
<tr>
<th>PRIVACY STANDARDS</th>
<th>DATA PROTECTION GLOBAL LEGAL MATRIX</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://arthrey.com">http://arthrey.com</a></td>
<td>[Table containing columns for Privacy Standards, Information Protected, Entities Covered by Law, and Privacy Official]</td>
</tr>
<tr>
<td><a href="http://eur.web">http://eur.web</a> offend.org</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.privireal.org">http://www.privireal.org</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://privacyexchange.org">http://privacyexchange.org</a></td>
<td></td>
</tr>
</tbody>
</table>

**INFORMATION PROTECTED**
- PHI: Protected Health Information
- Personally identifiable information
  - Directly or indirectly identifiable data
  - Personal Information (PII)
  - Personal Data (PD)
- Person: Personal Information about an identifiable individual but does not include name, address, business address or telephone number of an employee of an organization (business data).
- Individual: Also personal health information of a living individual not a corporation.

**ENTITIES COVERED BY LAW**
- Covered Entities: Health care providers, Health Insurance Plans and Healthcare Clearinghouses, their "HIPAA Business Associates," Personal Health Record Vendors.
- Data Controller and their Data Processors: Organization that collects, uses or discloses personal information in the course of commercial activity or personal information about an employee of a Canadian government entity or undertaking.
- "Business Holding Personal Information": By member state, e.g., Data Protection Commissioner - Germany, otherwise, by default, Managing Director of affiliate in practice.

**PRIVACY OFFICIAL**
- Privacy Officer
- Privacy Officer: senior management
- Privacy Contact / Privacy Officer
### DATA PROTECTION GLOBAL LEGAL MATRIX

<table>
<thead>
<tr>
<th>LAW / COUNTRY</th>
<th>U.S. - HIPAA 182</th>
<th>EU DATA PROTECTION</th>
<th>CANADA - PIPEDA</th>
<th>JAPAN - PIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ENFORCEMENT AUTHORITY</strong></td>
<td>Office of Civil Rights; State Attorneys' Generals; HITECH Act &quot;HIPAA 2&quot; mandated enforcement</td>
<td>European Commission; Data Protection Authorities of member states; US-EU Safe Harbor = US Federal Trade Commission</td>
<td>Commissioner of Privacy Commissioner of Canada - preferably through dispute resolution</td>
<td>Businesses must use best efforts to resolve complaints; within discretion of the competent Minister</td>
</tr>
<tr>
<td><strong>STAFF TRAINING REQUIRED</strong></td>
<td>Basic Privacy training on entities’ policies and procedures for HIPAA compliance - only for covered entities</td>
<td>Basic Awareness</td>
<td>Data Controller - person or body &quot;which determines the purposes and means of the processing&quot;</td>
<td>Basic Awareness; Advanced as appropriate</td>
</tr>
<tr>
<td><strong>DATA OWNER</strong></td>
<td>Those designated in Patient Authorization to use / disclose protected health information</td>
<td>Business Holding</td>
<td>&quot;Holder&quot; - Accountability - designate individuals accountable for compliance</td>
<td>Business Holding Personal information for purposes of use</td>
</tr>
<tr>
<td><strong>DATA RECIPIENT</strong></td>
<td>Health Care Provider, Health Plan, Healthcare Clearinghouse; their &quot;HIPAA Business Associates&quot;; Those designated in Authorization; IRBs, Regulatory / legal authorities</td>
<td>Not only Data Processor on behalf of Data Controller but any other third party with or without shared liability</td>
<td>Business Holding Personal information may delegate purposes of use, e.g., subcontractor - not regarded as third party</td>
<td></td>
</tr>
<tr>
<td><strong>DATABASE REGISTRATION WITH DATA PROTECTION AUTHORITY</strong></td>
<td>No; But &quot;accounting for disclosures&quot; required for disclosure by &quot;Covered Entity&quot; without individual's authorization</td>
<td>Notification of automatic processing operations (see Article 18 (1) EU Directive 95/46/EC)</td>
<td>N/A</td>
<td>PIPA applicable based on &gt;5000 entries collectively; no registration required</td>
</tr>
</tbody>
</table>

### DATA PROTECTION GLOBAL LEGAL MATRIX - CONTINUED

<table>
<thead>
<tr>
<th>LAW / COUNTRY</th>
<th>U.S. - HIPAA 182</th>
<th>EU DATA PROTECTION</th>
<th>CANADA - PIPEDA</th>
<th>JAPAN - PIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMPLIANCE REVIEWS</strong></td>
<td>Required as Safe Harbor - Random, periodic</td>
<td>Particularly for data transferred outside the EU pursuant to ODT and for sensitive data holdings</td>
<td>Recommend</td>
<td>Required</td>
</tr>
<tr>
<td><strong>EXTERNAL PENALTIES for VIOLATION</strong></td>
<td>Fine/Imprisonment for covered entities, their Business Associates, Personal Health Record Vendors, employees acting in &quot;bad faith&quot;. Most states and ORAs not a covered entity but clinical investigators are.</td>
<td>Specific to country; Fine/Imprisonment</td>
<td>Fine/Imprisonment</td>
<td></td>
</tr>
<tr>
<td><strong>SECURITY BREACH NOTIFICATION TO DATA SUBJECT / AUTHORITIES</strong></td>
<td>&quot;HIPAA 2&quot; Risk-Based Approach for Notification of Breach of PHI by Covered Entity and Personal Health Record (PHR) Vendor</td>
<td>Under consideration</td>
<td>Under consideration</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>EXCEPTIONS</strong></td>
<td>Public Safety, Law Enforcement, National Security</td>
<td>Public Safety, Law Enforcement, National Security</td>
<td>Public Safety, Law Enforcement, National Security, Research Publications</td>
<td>Public Safety, Law Enforcement, National Security, When consent is difficult to obtain</td>
</tr>
<tr>
<td><strong>OTHER</strong></td>
<td>Must meet requirements of certain state laws if not preempted by HIPAA</td>
<td>Must meet local country requirements of EEA/EU member states also</td>
<td>Must meet requirements of certain Canadian provinces if not preempted</td>
<td>Must meet provisions of certain Guidelines</td>
</tr>
</tbody>
</table>
# Data Protection Global Legal Matrix

<table>
<thead>
<tr>
<th>Law / Country</th>
<th>U.S. - HIPAA 182</th>
<th>EU Data Protection</th>
<th>Canada - PIPEDA</th>
<th>Japan - PIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy Principles:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notice / Acquisition</td>
<td>Provide Notice of Privacy Practices to Patients. For research requires specific Authorization (separate or included in Informed Consent).</td>
<td>Notification of Data Subject including information on how to exercise right of access and correction</td>
<td>Notice identifying purposes of use - balance need for information vs. right of privacy using reasonable person standard</td>
<td>Notify Data Subject upon acquisition, specify use of held data; disclosure; correction; cease of use</td>
</tr>
<tr>
<td>Purpose of Use / Identifying Purposes / Limiting Collection</td>
<td>Authorization - should explain purposes of use and categories of those to whom disclosed</td>
<td>Fair and Lawful: Explicit consent for sensitive personal data such as health information</td>
<td>Reasonable and appropriate - Limiting collection to that which is necessary to achieve purposes</td>
<td>Change of Use, cannot exceed the scope reasonably recognized as having an appropriate connection with original use. Business cards given special treatment</td>
</tr>
<tr>
<td>Choice (Consent - &quot;Opt In&quot; or &quot;Opt Out&quot;)</td>
<td>As applied in patient Authorizations or included in informed consents for access to Protected Health Information (PHI). Opt in for marketing</td>
<td>Informed consent if patient required for compliance. Opt in (specific consent to participate) for clinical trials but &quot;opt out&quot; (notify only if win opt to participate) such as for less sensitive uses as for business purposes - e.g., business surveys of customers.</td>
<td>Consent depends on sensitivity of personal information; usually required with exceptions for health information / clinical trials. Consent should be meaningful and freely obtained</td>
<td>Required for new use in maintaining personal information. Opt in (specific consent) for clinical trials but &quot;opt out&quot; for less sensitive use such as business purposes as in survey of customers</td>
</tr>
<tr>
<td><strong>Privacy Principles:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Onward Transfer to Third Party, Agents, or Outside the Country</td>
<td>No restrictions if for treatment, payment or health care operations. Otherwise, disclosure pursuant to &quot;Authorization&quot;, &quot;Privacy Notice&quot;, Contract, or &quot;HIPAA Exemption&quot;.</td>
<td>Outside of EU - must provide &quot;adequate level of protection&quot; - presumption of adequacy with certification to US-EU Safe Harbor; Data Transfer Agreements for transfer to other countries; Explicit Informed Consents, Binding Corporate Rules</td>
<td>Outside of Canada same as disclosure to third party agent, Data delegation agreements.</td>
<td>Outside of Japan same as disclosure to third party / agent. Data delegation agreements.</td>
</tr>
<tr>
<td>US-EU Safe Harbor Certification: Harboriste status - presumption of adequacy of protection for personal data transferred from EU to Harboriste entities in US</td>
<td>Privacy Statement posted publicly - Notice, Choice, Data Integrity, Transfers to Agents, Access and Correction, Security, Enforcement, Dispute Resolution</td>
<td>Privacy Statement posted publicly, Notice, Choice, Data Integrity, Transfers to Agents, Access and Correction, Security, Enforcement, Dispute Resolution</td>
<td>Canada is &quot;white listed&quot; country with mutual Memorandum of Understanding with EU for cross-border transfers of personal data. Accordingly, Canada may unilaterally recognize Safe Harbor.</td>
<td>Null through data protection procedures in US should be adequate for OJPN</td>
</tr>
<tr>
<td>Individual Access / Complaints</td>
<td>Access may be limited in Patient Authorization (until end of clinical study)</td>
<td>Must provide reasonable access to personal information and implement complaint procedures</td>
<td>Allow reasonable access / implement complaint procedures</td>
<td>Respond to Data Subject when asked to stop using data or other purpose than original use or to stop disclosure to third parties (opt out) but may refuse if too costly or difficult - while implementing alternative protective measures</td>
</tr>
</tbody>
</table>
### DATA PROTECTION GLOBAL LEGAL MATRIX

<table>
<thead>
<tr>
<th>LAW / COUNTRY</th>
<th>U.S. - HIPAA 182</th>
<th>EU DATA PROTECTION</th>
<th>CANADA - PIPEDA</th>
<th>JAPAN - PIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIVACY PRINCIPLES: SECURITY / SAFEGUARDS</td>
<td>Reasonable administrative and technical security measures</td>
<td>Reasonable administrative and technical security measures commensurate with risk to data subject</td>
<td>Implement measures to protect personal information in entity's control</td>
<td>Receive requests from Data Subject to correct personal data without delay, notify data subject whether request taken or reasons why not</td>
</tr>
<tr>
<td>PRIVACY PRINCIPLES: DATA INTEGRITY / ACCURACY (Correction)</td>
<td>Right to request correction</td>
<td>Complete, up-to-date and accurate</td>
<td>Complete, up-to-date and accurate</td>
<td>Accountability</td>
</tr>
<tr>
<td>PRIVACY PRINCIPLES: INTERNAL ENFORCEMENT</td>
<td>Covered entities should have written disciplinary measures for data protection violations “up to and including dismissal”</td>
<td>Procedures in place with disciplinary actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVACY PRINCIPLES: CESSION OR USE / TERMINATION / RETENTION</td>
<td>Right to restrict authorization for use and disclosure of person’s health information but not if it is needed as recipient already relied upon data</td>
<td>Retain for only so long as needed for purposes of use</td>
<td>Retention for so long as needed for purpose</td>
<td>Respond to Data Subject for Cession of use</td>
</tr>
</tbody>
</table>

### DATA PROTECTION GLOBAL LEGAL MATRIX

<table>
<thead>
<tr>
<th>LAW / COUNTRY</th>
<th>U.S. - HIPAA 182</th>
<th>EU DATA PROTECTION</th>
<th>CANADA - PIPEDA</th>
<th>JAPAN - PIPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFINITIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;HIPAA 1&quot; US - Health Insurance Portability and Accountability Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;HIPAA 2&quot; US - ARRAHITECH Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIPEDA Canada - Personal Information Protection and Electronic Documents Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIPA Japan - Personal Information Protection Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU - DP European Union Data Protection Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DTA EU Model Contracts - Data Transfer Agreement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHR US - HIPAA Protected Health Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NA = Not Applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions?