The EU GDPR:
Implications for U.S. Universities and Academic Medical Centers

Mark Barnes

ROPES & GRAY

February 21, 2018

Agenda

- **Introduction**
- Jurisdictional Scope of the GDPR Compared with the Directive
- “Offering Goods or Services” to Data Subjects in the EU
- “Monitoring Behavior” of EEA Residents
- Authority to Use and “Process” Personal Data
- Transfer of Personal Data to the U.S. and from U.S. to EEA
- Implications of GDPR’s Application to U.S. Universities and AMCs
- Recommended Steps

Introduction

- Effective May 25, 2018, the European Union's General Data Protection Regulation (the "**GDPR**") will make EU data privacy law much more rigorous and will broaden its jurisdiction.
- GDPR may apply extraterritorially to **U.S.-based universities and AMC**s", through, for example:
  - Online education programs;
  - Maintaining sites/study abroad branch sites in EEA member states;
  - Maintaining alumni clubs in and soliciting donations from EEA member states;
  - Recruiting students from EEA member states;
  - Maintaining patient referral arrangements with health care providers in EEA member states;
  - Offering telemedicine services to patients in EEA member states;
  - Sponsoring clinical research occurring in EEA member states;
  - Acting as a core data facility or lead site for a multi-national clinical trial with EEA-based sites; or
  - Study subject data are transmitted to sponsors, servers or data core facilities sited in the EEA.

Agenda

- Introduction
- **Jurisdictional Scope of the GDPR Compared with the Directive**
- "Offering Goods or Services" to Data Subjects in the EU
- "Monitoring Behavior" of EEA Residents
- Authority to Use and "Process" Personal Data
- Transfer of Personal Data to the U.S. and from U.S. to EEA
- Implications of GDPR's Application to U.S. Universities and AMCs
- Recommended Steps

GDPR and Superseded Data Protection Directive

- GDPR will supersede the presently effective EU Data Protection Directive, which was adopted in 1995. *See* EU Data Privacy Directive (Directive 95/46/EC) (the "**Directive**").
- The Directive and GDPR apply in the 28 member states of the EU and the three additional countries (Iceland, Liechtenstein and Norway) that together with the EU make up the European Economic Area ("**EEA**").
  - GDPR will apply directly across all of the EEA's member states, unlike the Directive, which supplied general principles that were implemented in a different fashion by each EEA member state.
  - The United Kingdom is preparing for GDPR implementation despite "Brexit."

Map of EEA Member States

EEA Members

EEA Member

Provisional EEA Member

European Free Trade Association ("EFTA") Members

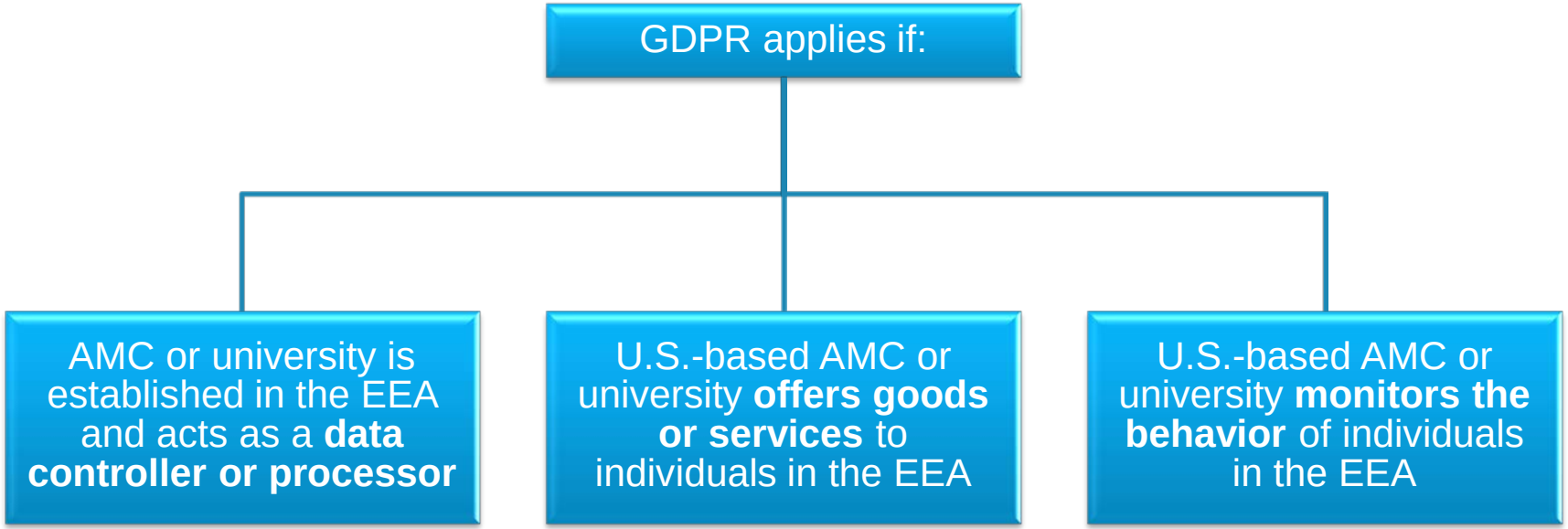
EFTA Member

EFTA Signatory, But Has Not Ratified

Current Directive's Application to U.S.-Based AMCs

- **GDPR will apply extraterritorially in a broader range of circumstances than the Directive.**
  - Typically, **the Directive has applied to U.S.-based universities and AMCs only in those scenarios in which a university or AMC is "established in" the EEA**.
  - A university or AMC could be deemed to be "established in" the EEA by virtue of:
    - Operating a subsidiary or campus in the EEA; or
    - Operating an office in the EEA.

GDPR Application to U.S.-Based AMCs



“Personal Data” under the GDPR

- “Personal data’’ are defined broadly to include:
  - “**[A]ny information relating to an identified or identifiable natural person** (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural, or **social identity** of that person.’’ (GDPR Art. 4(1)).
- “Special categories of personal data” include:
  - “[P]ersonal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership . . . genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.” (GDPR Art. 9(1)).

Data Subject to GDPR vs. HIPAA

- The set of data to which the GDPR applies is **broader than that covered under HIPAA**.
  - Applies to all "personal data" across all sectors of the economy, not only health care; no concept of "covered entity."
    - Personal data under the GDPR include, for example, identifying information on EEA health care providers (HCPs), such as principal investigators, and other persons who are not patients.
  - There is no anonymization "safe harbor" under the GDPR.
    - Identifiability is judged on a facts and circumstances test, taking into account "all the means reasonably likely to be used . . . [e]ither by the controller or by another person to identify the natural person directly or indirectly." (GDPR Recital 26).
    - "Pseudonymised" data (*e.g.* key-coded data) remain "personal data."

Controllers and Processors

- GDPR applies distinct requirements to two groups of entities:
  - A "**controller**" is an entity that, alone or jointly with others, determines the purposes and means of processing data.
    - *E.g.* acting as a collaborator as part of a research project.
  - A "**processor**" is an entity that processes personal data on behalf of the controller.
    - *E.g.* acting as a fee-for-service laboratory for a research project.

Agenda

- Introduction
- Jurisdictional Scope of the GDPR Compared with the Directive
- **“Offering Goods or Services” to Data Subjects in the EU**
- “Monitoring Behavior” of EEA Residents
- Authority to Use and “Process” Personal Data
- Transfer of Personal Data to the U.S. and from U.S. to EEA
- Implications of GDPR’s Application to U.S. Universities and AMCs
- Recommended Steps

Offering Goods or Services

- GDPR provides that, "[i]n order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor **envisages offering services to data subjects** in one or more Member States in the Union." (GDPR, Recital 23).
  - GDPR notes that the goods or services offered should be considered "**irrespective of whether connected to payment**." (GDPR, Recital 23).
- Little guidance has been offered on the meaning of "offering goods or services" to persons located in the EEA.

Offering Goods or Services

- GDPR clarifies that "**mere accessibility of the controller's, processor's or an intermediary's website**" in the EEA is **insufficient to ascertain an intention to offer goods or services in the EEA**. (GDPR, Recital 23).
  - GDPR jurisdiction therefore requires that a website be somehow **directed to EEA data subjects**, such as translating the website into an EEA member state language, using an EEA member state currency, or mentioning customers or users in the EEA. (*See* GDPR, Recital 23).
  - **This is effectively a low bar to GDPR's jurisdiction/application to U.S.-based entities, including universities and AMCs.**

U.S. Universities Offering Goods or Services

- Arrangements and practices that might be seen as a U.S. university "envisioning" providing services to EEA data subjects:
  - "Study abroad" programs
  - Recruiting that targets students in EEA member states.
  - Recruiting visiting faculty and/or fellows.
  - University publishing house targeting customers in EEA member states.
  - Collaboration agreements with universities in EEA member states to develop educational platforms and share data.

U.S. AMCs Offering Goods or Services

- Arrangements that might be seen as a U.S. university or AMC "envisioning" providing services to EEA data subjects.
  - Referral arrangements between U.S. AMCs and EEA HCPs involving a written agreement for referral of patients.
  - Consultation arrangements in which the U.S. AMC offers consultation services to EEA HCPs.
  - Third and fourth year medical student rotations in EEA-based hospitals/clinics.
- In the above scenarios, the EEA "data subject" whose data are subject to GDPR could include **both the EEA HCP and the EEA patient**.

U.S. Universities or AMCs Offering Goods or Services

- If a university or AMC does not target its website to EEA data subjects, conduct other advertising targeted at EEA residents, or establish routine relationships with EEA residents, the university or AMC may be able to argue that it does not "offer goods or services" to EEA data subjects within the meaning of GDPR.
- Thus, for example, the GDPR may not apply to:
  - AMC providing occasional treatment to patients from the EEA who travel to the U.S. to seek services at the AMC; or
  - AMC's providers engaging in occasional informal consultation with EEA health care providers.

U.S. Universities or AMCs Offering Goods or Services

- Research arrangements involving **European governmental grants or contracts.**
  - U.S. universities or AMCs may be direct awardees or sub-recipients through EEA institutions of European governmental grants or contracts to perform research services.
  - Terms of grant may require compliance with GDPR.
  - Personal data flows to and from EEA direct grant awardees should be scrutinized to see if they "envisage" offering services to EEA data subjects.

Agenda

- Introduction
- Jurisdictional Scope of the GDPR Compared with the Directive
- “Offering Goods or Services” to Data Subjects in the EU
- **“Monitoring Behavior” of EEA Residents**
- Authority to Use and “Process” Personal Data
- Transfer of Personal Data to the U.S. and from U.S. to EEA
- Implications of GDPR’s Application to U.S. Universities and AMCs
- Recommended Steps

GDPR Recitals on “Monitoring Behavior”

- GDPR’s recitals provide that “[i]n order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained **whether natural persons are tracked on the internet** including potential subsequent use of personal data processing techniques which consist of profiling a natural person, **particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviors and attitudes.**” (GDPR, Recital 24).

“Monitoring Behavior” and Education

- Certain university operations may involve “monitoring behavior” of EEA data subjects:
  - Online education programs that include participants from EEA member states and use cookies to track student participation.
  - Educational records (*e.g.* attendance, participation and grades) compiled at U.S.-based universities’ European satellite campuses.
  - Tracking giving history of alumni and other donors in EEA member states.

“Monitoring Behavior” and Clinical Trials/Human Subjects Research

- Conducting clinical research with research sites or research subjects located in the EEA could involve activities that may constitute ‘‘monitoring of the behavior of data subjects.’’
  - Multi-Site Research: U.S. university or AMC that serves as a lead site for a clinical trial with sites located in the EEA could be seen as monitoring the behavior of data subjects in the EEA if the university or AMC is required to monitor research subject records for adverse events.
  - Mobile Application Research: U.S. universities or AMCs may conduct research studies through mobile applications whereby the university or AMC enrolls subjects in the study remotely and the app collects data on the subject’s physical condition or geographic location through the subject’s mobile phone. If such studies target individuals in EEA member states, this activity could be seen as “monitoring behavior” of data subjects in the EEA.

“Monitoring Behavior” and Telemedicine

- While the GDPR’s recitals focus on tracking behavior through the internet, telemedicine offered by a U.S.-based physician to a patient located in the EEA would seem to constitute “monitoring behavior.”
  - Could also be interpreted as offering a good or service to the data subject

Agenda

- Introduction
- Jurisdictional Scope of the GDPR Compared with the Directive
- “Offering Goods or Services” to Data Subjects in the EU
- “Monitoring Behavior” of EEA Residents
- **Authority to Use and “Process” Personal Data**
- Transfer of Personal Data to the U.S. and from U.S. to EEA
- Implications of GDPR’s Application to U.S. Universities and AMCs
- Recommended Steps

Authority to Use and “Process” Personal Data

- Bases for processing **personal data** include:
  - Data subject has given **consent** to processing.
  - Processing necessary for the **performance of a contract** to which the data subject is a party.
  - Processing necessary for **compliance with a legal obligation.**
  - Processing necessary to protect **vital interests** of the data subject or a natural person.
  - Processing necessary for a **task carried out in the public interest.**
  - Processing necessary for the **legitimate interests of the controller** or a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject.

    (GDPR, Art. 6(1)).

Authority to Use Special Categories of Personal Data

- Bases for processing **special categories of personal data** include:
  - **Explicit consent** of the data subject to processing.
    - Article 29 Working Party: "'explicit consent' is understood as having the same meaning as **express consent**." (Opinion No. 15/2011 (WP197) of the Article 29 Data Protection Working Party).
      - Express consent "encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, **explicit or express consent is given in writing with a hand-written signature**." (*Id.*).
    - But EU or Member State law may provide that the data subject may not provide valid consent to certain processing of special categories of personal data. (GDPR Art. 9(2)(a)).
  - Processing necessary to protect the **vital interests** of the data subject or another natural person **where the data subject is physically or legally incapable of giving consent**.
  - Processing necessary for reasons of **public interest in the area of public health**.
  - Processing necessary for **scientific or historical research purposes**.

    (GDPR Art. 9(2)).

Agenda

- Introduction
- Jurisdictional Scope of the GDPR Compared with the Directive
- “Offering Goods or Services” to Data Subjects in the EU
- “Monitoring Behavior” of EEA Residents
- Authority to Use and “Process” Personal Data
- **Transfer of Personal Data to the U.S. and from U.S. to EEA**
- Implications of GDPR’s Application to U.S. Universities and AMCs
- Recommended Steps

Requirements for Transfer of Personal Data to U.S.

- Both the Directive (currently in effect) and GDPR (upon its implementation) **require that a legal basis be in place to permit the transfer of personal data from the EEA to jurisdictions lacking adequate data protection legislation (*e.g.*, the United States)**. (*See* Directive Ch. IV; GDPR Ch. V).
- Even if a U.S. university or AMC's activities do not subject it directly to regulation under the GDPR, certain steps may be required to ensure that an adequate legal basis exists to permit the transfer of data from the EEA to the U.S., for example:
  - A research collaborator in the EU transfers files of pseudonymised (coded) data to the U.S. university or AMC for research purposes.
  - A patient who is an EEA resident falls ill while on vacation in the U.S. and the AMC treating the patient requires medical records from the patient's primary care physician in the EEA to assist in treatment.

Legal Bases for Data Transfer to US

- Obtaining the **explicit consent** of the data subject to the transfer of personal data to the U.S. for processing.
  - Requires **advising the data subject of the risks** of the transfer resulting from the absence of adequate data protection legislation in the recipient jurisdiction.
  - May work well in the context of clinical care or prospective clinical research, in which consents are customarily obtained.
- Entering into **model contractual clauses** approved by the European Commission with the EEA entity transferring personal data to the university or AMC, such as the European hospital or research institute that is transferring information. Model clauses impose on the contracting U.S.-based university or AMC certain of the requirements of EU data privacy law with respect to the data transferred under the contract.
- Data transfers necessary to protect the "**vital interests**" of the data subject.
  - Generally considered to be "life and death" situations.

Legal Bases for Data Transfer to US

- U.S.-based universities or AMCs that are **for-profit entities** may have an additional option of applying for certification under the **EU-U.S. Privacy Shield**, a program administered by the U.S. Department of Commerce.
  - Permits personal data to be transferred from the EEA to U.S. for-profit entities that self-certify for the program after implementing various data protection measures consistent with EU privacy law.
- Associations may create **codes of conduct** setting forth rules on data processing. Such codes must be approved by the supervisory authority in the relevant EEA jurisdiction or the European Data Protection Board, if operable in multiple jurisdictions.

Personal Data in the Reverse Direction: Personal Data Transferred from US to EEA

- There are potential implications of the GDPR with respect to **the transfer of personal data from the U.S. to the EEA,** for example, for clinical research sponsored by EEA-based companies or for which an EEA-based AMC serves as lead site or data coordinating center.
  - U.S. university or AMC may need to transfer its employees' data to the EEA if the university or AMC is serving as a clinical trial site for an EEA-based clinical research sponsor, such as an EEA-based pharma company or AMC.
    - EEA-based research sponsor may request that the U.S. entity's employees sign a consent form to allow processing of their data in the EEA.
    - EEA-based research sponsor may need to provide a notice regarding data processing activities to the U.S. entity's employees whose data are being transferred to EEA sponsor.

Personal Data Transferred from US to EEA

- U.S. university or AMC may need to transfer clinical trial data of research subjects to the EEA when the **trial is sponsored by an EEA-based entity or EEA-based entity serves as the lead site**.
  - EEA-based sponsor may need the US AMC to obtain trial subjects' consent that meets the notice requirements of the GDPR and permits processing of their data in the EEA.
  - Consent will likely need to include the following information not usually included in consent forms used for U.S. subjects:
    - Fact that data will be transferred to EEA for analysis
    - Identity of data controller/Data Protection Officer
    - Contact information for data subject to file complaints with applicable data protection authority

Personal Data Transferred from US to EEA

- Additional elements required for a GDPR-compliant consent:
  - Period for which data will be maintained or criteria used to determine the period
  - Rights to:
    - Object to processing
    - Request rectification of data
    - Request portability of data
    - Request erasure of data

Agenda

- Introduction
- Jurisdictional Scope of the GDPR Compared with the Directive
- “Offering Goods or Services” to Data Subjects in the EU
- “Monitoring Behavior” of EEA Residents
- Authority to Use and “Process” Personal Data
- Transfer of Personal Data to the U.S. and from U.S. to EEA
- **Implications of GDPR’s Application to U.S. Universities and AMCs**
- Recommended Steps

Implications if GDPR Applies

- GDPR imposes requirements on data processing and grants rights to data subjects that exceed those found under HIPAA.
  - Consider whether university or AMC knows identity of subject or receives only pseudonymised data.
- GDPR provides for a **broader data subject access right** than does HIPAA. (*See* GDPR Art. 15; 45 C.F.R. § 164.524).
  - GDPR generally allows data subjects to obtain copies of **all of their personal data** undergoing processing.
  - In contrast, HIPAA provides a right of access **only to protected health information stored within a covered entity's "designated record set."**
  - GDPR does **not** contain exceptions found in HIPAA to the access right for certain categories of PHI, such as:
    - Psychotherapy notes; or
    - PHI collected during a research study, provided that the subject agreed to the suspension of the right of access for the pendency of the research

Implications if GDPR Applies

- GDPR provides the data subject the right to obtain **additional information in an accounting of disclosures**, including the source of the personal data if the source is not the data subject himself/herself. (*See* GDPR Art. 15; 45 C.F.R. § 164.528).
- GDPR contains a "**right to erasure**," also known as a "**right to be forgotten**," that permits the data subject to **request that data be erased when certain circumstances apply**, including the following:
  - Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - Data subject withdraws consent on which the processing is based;.
  - Data subject objects to processing that was based on legitimate interest of the controller and the controller cannot demonstrate compelling legitimate grounds for the processing;
  - Personal data have been unlawfully processed; or
  - Personal data have to be erased for compliance with a legal obligation in EU or member state law to which the controller is subject. (*See* GDPR Art. 17).

Implications if GDPR Applies

- GDPR requires non-EU data controllers and processors subject to the GDPR to **appoint an EU representative** unless their processing is occasional and certain other requirements are met. (*See* GDPR Art. 27).

Implications if GDPR Applies

- Data subjects must be provided a **notice** at the time their data are collected setting forth several details not typically found in a HIPAA notice of privacy practices or a HIPAA-compliant research authorization:
  - Identity and contact details of controller and controller's EU representative
  - Purposes and legal basis for processing data under EU law
  - Period of time for which data will be stored or criteria used to determine period
  - Right to request erasure of personal data
  - Right to lodge complaint with EU data protection authorities
  - Any "automated decision-making" made on the basis of the processing

  (*See* GDPR Art. 13)
- Notice could be provided to patient at time of treatment or included in a research consent form.

Implications if GDPR Applies: Penalties

- With respect to enforcement penalties, **fines from infringements under the GDPR can be extensive**. (*See* GDPR Art. 83).
  - Fines up to the higher of € 10,000,000 or 2 percent of worldwide annual turnover for the violation of some GDPR Provisions.
  - Fines of the higher of € 20,000,000 or 4 percent of worldwide annual turnover for violation of other provisions, including the provisions on subject access and right to erasure.
- Unlike HIPAA, GDPR confers a **private right of action on data subjects**, who may bring damages claims directly against data controllers and processors. (*See* GDPR Art. 82).
  - In some jurisdictions, including the United Kingdom, individuals need only show distress in order to claim financial damages—financial loss is not a determinative factor in the risk analysis.

Agenda

- Introduction
- Jurisdictional Scope of the GDPR Compared with the Directive
- “Offering Goods or Services” to Data Subjects in the EU
- “Monitoring Behavior” of EEA Residents
- Authority to Use and “Process” Personal Data
- Transfer of Personal Data to the U.S. and from U.S. to EEA
- Implications of GDPR’s Application to U.S. Universities and AMCs
- **Recommended Steps**

Recommendations

- Universities and AMCs should **monitor whether EU regulatory bodies issue further guidance** clarifying the circumstances in which the GDPR applies to trans-national treatment, research and health care operations activities.
- Universities and AMCs should **identify the circumstances under which they receive and process personal data** from, or generate personal data in, the EEA.
  - Begin with a fact gathering exercise to determine all relevant data flows.
  - Outline of relevant questions is presented on the following slides.

Recommendations – Fact Gathering

Advertisements and Recruiting

- What advertising, recruiting, or public relations activities does the university or AMC undertake in the EEA?
- Is the university or AMC's website translated into EEA member state languages?
- Does the university or AMC's website direct itself to EEA residents, such as through quoting prices in local currencies, profiling EEA residents who have been students or patients, or advertising academic or referral arrangements with with EEA-based HCPs/AMCs?
- Does the university press market its publications to customers in the EEA member states?

Recommendations – Fact Gathering

Education-Related Activities

- Does the university maintain campuses, offices or other sites in EEA member states, such as in connection with study abroad programs?
- Does the university offer online classes translated into languages of the EEA member states or that otherwise could be said to target residents of the EEA member states?
- Does the university coordinate programs for alumni in the EEA member states?
- Does the university track or solicit donations from alumni or other donors in the EEA member states?

Recommendations – Fact Gathering

Patient Care Activities

- Does the AMC offer telemedicine or second opinion services to patients in the EEA?
- Does the AMC have any affiliation or referral arrangements with EEA HCPs?
- Does the medical school or other professional school offer rotational placements in EEA-based health facilities?
- Does the AMC permit any EEA HCPs to operate under the AMC's "brand"?

Recommendations – Fact Gathering

Research Activities

- Does the university or AMC serve as a lead site for research activities taking place at EU sites, such as acting as a prime recipient of an NIH grant which flows through sub-awards to EU sites?
- Does the university or AMC conduct any studies involving mobile applications that target enrollment in the EEA?
- Does the university or AMC conduct industry-sponsored studies for companies located in the EEA, with personal data of U.S. residents being sent to and/or processed in the EEA?

Recommendations – Fact Gathering

Bases for Legitimizing Personal Data Transfers From EEA to U.S.

- Does the university or AMC have compliant consent forms that legitimize the transfer of personal data from the EEA to the U.S. with data processing occurring in the U.S., or from U.S. to EEA with data processing occurring in EEA?
- Has the university or AMC entered into model contractual clauses with EEA institutions from which AMC receives personal data?
- Is the university or AMC eligible for Privacy Shield certification?
- Is there a “code of conduct” to which the organization can adhere that would serve as a basis to legitimize the data transfer?

Recommendations – Implementation

- If U.S. university or AMC determines that its activities are subject to the GDPR, implementation steps would include the following (non-exhaustive list):
  - **Determine legal bases for processing personal data and special categories of personal data (*e.g.*, consent, vital interest).**
  - Draft notices of data processing activities advising subjects of purposes of processing, recipients of data, and the subject's rights.
  - Develop processes for responding to data subject requests (*e.g.*, request for access, rectification, restriction on processing, data portability).
  - Appoint a Data Protection Officer if processing special categories of personal data or conducting regular and systematic monitoring of subjects.
  - Appoint an EU representative (unless processing is only occasional, does not include large scale processing of sensitive personal data, and is unlikely to result in a risk to the rights and freedoms of natural persons).

Recommendations – Implementation

- Develop procedure for maintaining records of processing activities and consents for processing.
- Develop breach reporting procedures, *i.e.*, reporting to EU supervisory authorities and data subjects.
- Update vendor contracts to implement GDPR requirements for entities processing data on behalf of the university or AMC.
- Implement appropriate technical and organizational security measures (harness existing HIPAA Security Rule infrastructure).

Recommendations – Implementation

- Analyze basis for legitimizing transfer of personal data from EU to the U.S., *e.g.*:
  - Model contractual clauses
  - Consent
  - Binding corporate rules
  - Privacy shield (not applicable to not-for-profit entities)
  - Codes of Conduct? (possible future state)

The EU GDPR:
Implications for U.S. Universities and Academic Medical Centers

Mark Barnes

ROPES & GRAY

February 21, 2018