THE EVOLUTION OF HIPAA REGULATION

- **HIPAA enacted**: 1996
- **Transactions Standards & Privacy Rule**: 2000
- **Security Rule**: 2003
- **Enforcement Rule**: 2006
- **Breach Notification Interim Final Rule & HITECH Act**: 2009
- **Omnibus Rule**: 2013
WHO IS REQUIRED TO COMPLY?

• **Covered Entities**
  • Health care provider who electronically conducts a covered transaction (e.g., electronically bills insurers)
  • Health plan
  • Health care clearinghouse

• **Business Associates**
  • Creates, receives, maintains or transmits
  • Protected health information
  • On a covered entity’s (or another business associate’s) behalf
• Health information:
  • Relates to the past, present or future physical or mental health or condition of an individual;
  • Provision of health care to an individual; or
  • Past, present or future payment for the provision of health care to an individual

• Individually identifiable unless:
  • Expert Determination Method: Expert determines very small risk of identifiability; or
  • Safe Harbor Method: 18 identifiers removed (including dates related to individual (other than year), zip codes and smaller, any unique identifiers)
DE-IDENTIFICATION: SAFE HARBOR METHOD

“The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”
A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination.
Health Data Privacy Issues & Outlook

Webinar -- HIPAA: Privacy, Security and New Challenges, Oh My!

Andrew Fish
Chief Strategy Officer, AdvaMed
**Mission:** To develop and promote public policies and best practices that advance health care through digital health innovation and adoption.

The AdvaMed Center for Digital Health promotes the critical role of data and digital medical technologies in transforming health care. The Center advocates for public policies and best practices that advance digital health innovation and adoption and build trust among all stakeholders.

As a thought leader and convener, the Center for Digital Health is home to a wide range of medical and digital technology companies that are driving transformative advances in digital health that enable new insights, support health and wellness, improve patient interventions and outcomes, and enhance the efficiency of health care delivery.

Center for Digital Health member companies are innovators throughout the health care ecosystem, including medical device, digital therapeutic, pharmaceutical, and consumer and data technology companies.
Our Take on Digital Health

We take a broad view of digital health, not as a vertical but rather as an evolving complement of digital technologies and data capabilities that are increasingly embedded across medical technology and health care. As a wide range of stakeholders, including health care providers, patients, and consumers, adopt and integrate digital health technologies, the net effect is increasingly efficient delivery of higher quality patient care and improved patient outcomes. The digital health revolution encompasses:

- **Data-generating and communications technologies** that:
  - Diversify and improve data collection and communications platforms within and outside of traditional, intensive health care settings through telehealth, encounter-based technologies, wearables, ingestibles and implantables to –
  - Enable collection of novel, real-time, more frequent, and/or continuous information that –
  - Yield new scientific insights into health and disease states (population and individual), enables remote or on-site monitoring and interventions, and empowers consumers and patients.

- **Aggregation, analysis and use of data** to advance scientific understanding; inform health care decision making; support research and development; facilitate product approvals and regulatory compliance; administer and evaluate value-based care; improve delivery and quality of care, including patient experience; and empower remote and/or automated interventions.

- **Data-driven technologies** that:
  - Inform and/or augment human decision making, and
  - Effect remote and/or automated interventions.
Health Data (R)Evolution

Health Data Growth in Multiple Dimensions
(e.g., volume, type, site of collection, controlling entities, etc.)

+ Data Capabilities
  (e.g., AI)

= Patient & Stakeholder Value
  
  New Business Models (e.g., unscaling)
  
  Improved Care Delivery & Outcomes (e.g., diabetes closed loop systems)
  
  Disaggregated Care (e.g., remote monitoring)
  
  Enhanced Data Sharing/Interoperability (e.g., patient EHR access)
  
  Etc.

But Also

Policy & Operational Challenges

Privacy
Security
Trust
Health Data Privacy – AdvaMed Principles*

The collection, sharing and use of health information is fundamental to advancing health care, and holds the promise of delivering higher quality care and better health outcomes at lower overall cost. It is essential that U.S. privacy policy foster continued innovation in health care, while assuring individuals that personally identified data used for health-related purposes (“personal health data”) is subject to meaningful privacy safeguards.

U.S. data privacy policy should:

- Harmonize privacy requirements and standards nationwide to ensure clarity, consistency, predictability, and efficient compliance and oversight, taking into account existing regulatory frameworks for personal health data and deidentified health data.

- Take into account the unique nature and widely varied, complex uses of personal health data and deidentified health data to ensure that their utility is not unduly limited, including with regard to cross-border sharing and use.

- Incorporate a risk-based approach to both personal health data and deidentified health data, such that privacy obligations and protections are proportional to the sensitivity of data and do not unduly constrain important uses of data to improve health care.

- Establish a comprehensive and practical approach to notice and consent regarding the collection and use of personal health data.

- Ensure that individuals have reasonable access to their personal health data from the entity with primary responsibility for the original purpose for which the data was collected.

- Reserve oversight and enforcement to federal authorities with appropriate privacy expertise.

Privacy Regulation – Status and Outlook

Areas of AdvaMed Engagement & Monitoring

➤ U.S. States
  • Numerous more narrow bills introduced or passed (e.g., biometric data)
  • AdvaMed supporting uniform exemptions for certain categories of health data (adopted in VA, NY, FL, WA and piecemeal in CA)
  • **Key Point:** In absence of new federal law, state legislative momentum will continue or grow

➤ U.S. Federal
  • Congress
    o Multiple introduced bills and hearings; general bipartisan/bicameral alignment on numerous substantive points with preemption and private right of action as major sticking points; wide industry support for comprehensive federal law
    o **Key Point:** Comprehensive federal privacy law is closer than ever, but still uncertain – treatment of health data an open question
  • Agencies: HIPAA reforms; interoperability; information blocking / ONC: *Health Interoperability Outcomes 2030* / FTC: examining rulemaking
    • **Key Point:** Multiple statutes give federal agencies authority to adopt new policies on aspects of health data privacy, accessibility, and use

➤ Global
  • Cross-Border Data Flows (EU: Post-*Schrems II* fallout, Privacy Shield, Standard Contractual Clauses; China: new draft privacy law)
  • **Key Point:** Emerging enforcement activity + Distrust + Tech backlash + Value of data = Nationalization/Localization = Constraints on innovation
U.S. Health Privacy Regulation – Key Challenges

Two Essential Priorities in Tension: Protect Personal Privacy & Foster Innovation

- Personal health information is among the most intimate data, which necessitates appropriate safeguards, but it is also among the most valuable data because its use expands medical knowledge, drives technology innovation, and improves health care and patient outcomes.

Some (But Not All) Essential Questions

- Is HIPAA still ‘fit for purpose’?
- How to address health data outside the scope of HIPAA?
- What are the implications of having multiple frameworks for health data depending on entity, purpose, origin, etc.?
- Should health data be differentiated in general privacy legislation? (exemptions/additional protections/latitude for critical uses of identified/identifiable data, etc.)
- Is HIPAA a federal precedent for addressing a full scope of health data under a dedicated privacy framework?

Thank You
The businesses of Merck KGaA, Darmstadt, Germany operate as EMD Serono, MilliporeSigma and EMD Electronics in the U.S. and Canada.

PHI and the European GDPR

Webinar -- HIPAA: Privacy, Security and New Challenges, Oh My!

Joerg Steinhaus, Group Data Privacy Officer
26 May 2021
Since our founding over 350 years ago, we’ve become truly global with more than **58,000 employees in 66 countries** working on breakthrough solutions and technologies.

In the U.S. and Canada, we operate as EMD Serono in the Healthcare business, MilliporeSigma in the Life Science business, and EMD Electronics in the high-tech materials business.
58,000
Employees worldwide

17.5
Sales (€ billion) in 2020

66
Countries

1668
Founded

2.3
R&D (€ billion)

HIPAA and EU Data Privacy | 26 May 2021
INTERNAL POLICIES

Internal Policies and Procedures on the handling of Personal Data (PII)
WE ARE EVOLVING OUR GLOBALLY OPERATING DATA PRIVACY MANAGEMENT SYSTEM

WHAT WE WANT TO ACHIEVE

... ensure that our business activities are in line with external regulations

... strengthen a consistent global DP standard & application for all countries, sectors and functions

WHAT WE ARE PLANNING

Portfolio
GLOBALLY IMPLEMENTED DP PROGRAM AND PROCESSES

People
TRANSFORM AND GROW THE TEAM

Communication
DP AWARENESS AND HELPFUL COMMUNICATION MATERIALS
Our challenges as a European-based enterprise

**Scientific research**
- New developments based on research and clinical trials
- EU CTR now applicable

**International transfer**
- Data transfer outside the EU
- Cross-border research limited in many cases

**De-identification**
- HIPAA concept not known in EU
- Pseudonymization and anonymization not clear

**Data Minimization**
- Reduce PII to minimum required for a specific purpose
- Inform individuals about data use

**Exchange of data**
- We do not sell data. There is exchange of PHI only within our operations, and with partners under business agreements
There are various kinds of personal data

EXAMPLES

- Name
- Address/location
- Telephone
- National identification number
- Online identifiers
- Date of birth

GREATER PROTECTION for special categories such as

- Health data
- Genetic data
- Biometric data
- Political opinion
- Membership in a union
- Religious beliefs

We structure personal data into various data types:

- Customers
- Patients
- Employees
- Processors / Third Party
- Health Care Professionals
- Miscellaneous
We follow six key principles to ensure compliant handling of personal data

**Lawfulness**
- Processing of personal data must adhere to existing laws
- Reasons for processing must be documented in the DP tool

**Fairness**
- Respect the interest of individuals when working with personal data
- Responsibilities for the processing of personal data must be defined by the process owner in the DP tool

**Transparency**
- Be open with what you are doing. Individuals should be informed about our data use in clear and plain language
- Data must be stored accurately and corrected if wrong or outdated

**Purpose**
- Every processing requires a specific, clearly defined purpose
- Purposes should not be too broad or lead to excessive data processing
- Purpose changes must follow the six DP principles again

**Relevance**
- Only collect personal data which you really need
- Store personal data only as long as needed for the specific purpose or stated by law

**Safeguards**
- Store/Process personal data in a secured environment only
- Data should only be accessible to authorized persons
INTERNATIONAL DATA TRANSFER

Data transfers after Schrems II-decision
Limitations to international (cross-border) data transfer

**RISKS**
- Global effect from ECJ decision for entities from the EU, but focus on transfer between US and EU
- Many solutions provided by different authorities, but **no structured approach**

**SOLUTIONS**
- New set of EU Standard Contractual Clauses (SCC) expected soon
- **Privacy shield** 3.0 rather uncertain
- Discussions in potential US-EU Tech and Trade Council
DE-IDENTIFICATION AND ANONYMIZATION

A proposal for an EU Industry Code of Conduct
**EU GDPR Limitation though in research and development**

- No concept in Europe for de-identification of PHI
- Pseudonymization not sufficient to extend the purpose of research
- Anonymization not defined

**Need for de-identification concept**

**SECONDARY USE OF CLINICAL TRIAL DATA**

- Use of personal data from clinical trials limited to the original purpose under EU GDPR
- Clinical trial data not personalized, but key-coded

**DOUBLE PSEUDONYMIZATION**

- Possible solution with industry best practice in an authority-approved Code of Conduct
Rationale for proposed Code of Conduct  
(Source: EFPIA)

1. A GDPR Code of conduct would enable the sector to identify key data protection challenges and align on key data protection positions, thereby providing more clarity and certainty for clinical research. It would also provide certainty to third parties, including data subjects.

2. If we take the opportunity, it will facilitate access to data, accelerate research and contribute to us being better able to respond to patient needs.

3. The Covid-19 pandemic has served to move the case for action from strong to overwhelming.

4. The code would also clarify the linkages between the GDPR and other key sectoral legislation such as the Clinical Trials Regulation and would respond to the Commission’s policy ambitions for the European Data Space.

5. Patients will have stronger assurances and clarity with regards to the way their personal data is protected and processed by pharmaceutical companies that adhere to the Code.
**Our Key Learnings**

**Harmonization**
- Better understanding of rules and **more consistency** for companies
- **Better predictability** leads to more long term-developments, e.g., in pharmaceutical industry
- Gives more **clarity to individuals** and helps them to control their data

**Self-Governance**
- Comes out of industry’s needs, e.g., with **anonymization** concept
- Requires **a framework** to built on (like EU GDPR or a US federal bill)
- Provides **clear rules**, but leads to flexibility to grow new ideas

**Political Support**
- **International data transfer** nearly impossible without political will
- Based on provision of safeguarding instruments, like **new SCC** or new US-EU privacy shield
- New initiatives like **US-EU Tech and Trade Council** for broader view
DATA PRIVACY

PROTECTING OUR COMPANY

by handling personal data responsibly