MEDCON
CONFERENCE
Columbus, OH • April 24-27, 2023
CO-SPONSORED BY THE FDA

Security and Privacy

April 25, 2023

AFDO RAPS HEALTHCARE PRODUCTS COLLABORATIVE

MEDCON CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

Overview and Key Concepts

Regulatory Landscape

U.S. Federal:

FDA, HIPAA, FTC Act

Other privacy laws include GLBA, FERPA, FCRA, CAN-SPAM, TCPA, COPPA, cyber information sharing laws

U.S. State Laws:

Comprehensive: California, Virginia, Colorado, Connecticut, Utah, Iowa.

Data Breach Notification

Consumer Protection

Assorted Security

International: GDPR (EU/UK), PIPEDA (Canada), others.

Issue Spotting: Privacy Obligations

- Privacy laws create varied obligations regarding the collection and processing of personal data.
- Examples include:
  - Notice to consumers regarding how their personal information is being collected, shared and used;
  - Limits on how such data can be shared; and
  - Ensuring adherence to “minimum necessary” principles.

Issue Spotting: Personal Information

- **Personal Information (CCPA):**
  - "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
- **Personal Information (CPA/VCDPA):**
  - "information that is linked or reasonably linkable to an identified or identifiable natural person."
- **Personal Data (GDPR)**:
  - "any information relating to an identified or identifiable natural person."
- **Personally identifiable information (PII):**
  - narrower that "personal information" and includes specific elements of information
  - used in the context of security/breach

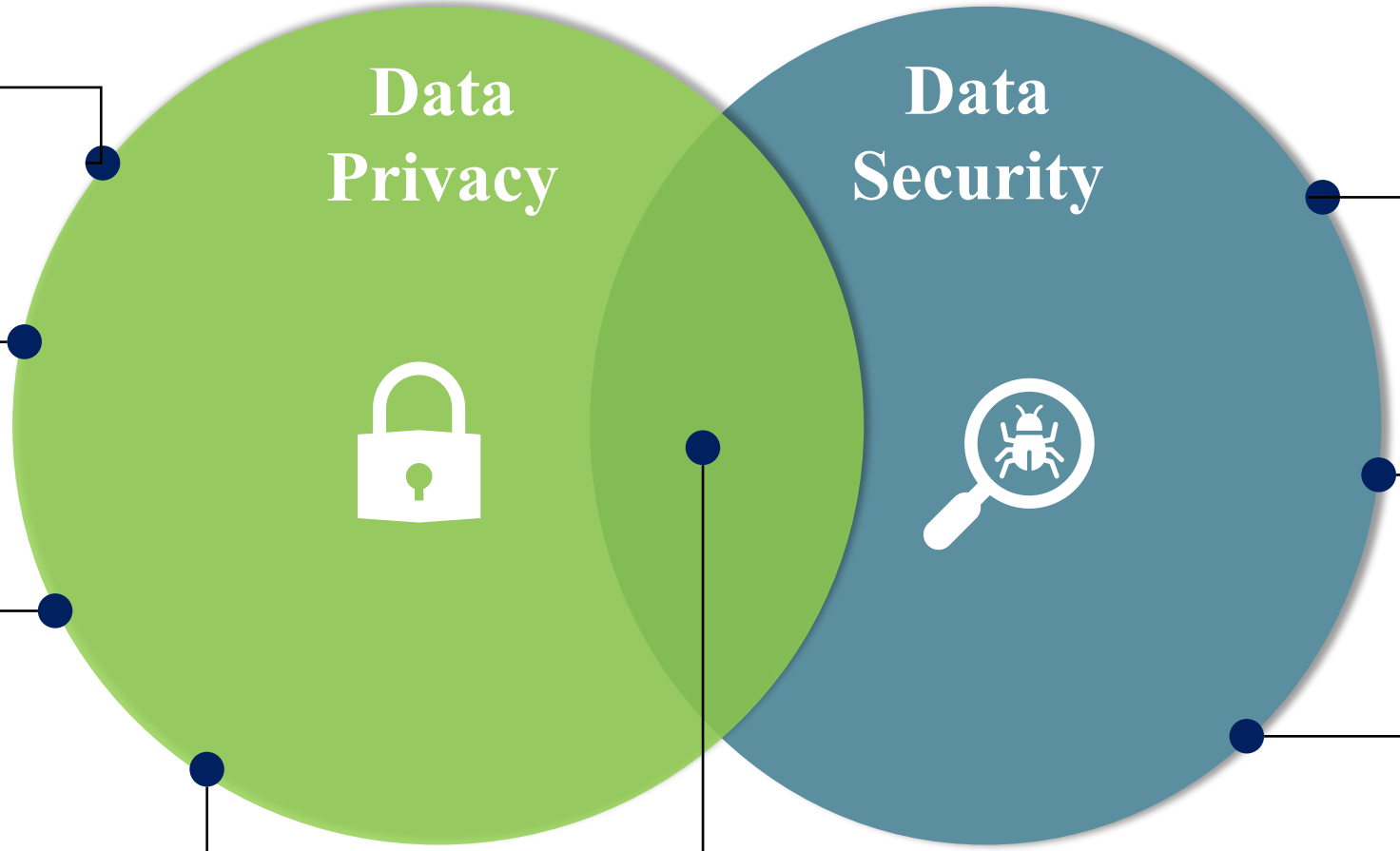
Issue Spotting: Data Controllers / Processors

- **Data Controller (GDPR, VA, CO)**:
  - "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"
- **Data Processor (GDPR, VA, CO)**:
  - "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"
  - CCPA uses the term "service provider" for a similar concept.

Issue Spotting: Data Subject Rights

- **Data Subject:** The natural person who is the subject of the personal data.
- **Data Subject Rights:** Privacy and security laws grant data subjects rights pertaining to their personal data.

Issue Spotting: Data Protection Program



Collection
How is Personal Information Collected

Use
How is Personal Information Used

Disclosure
Who Has Access to Personal Information

Accuracy
How Accurate is the Personal Information

Protection
Keeping Personal Information Secure

Confidentiality
Protecting Data from Unauthorized Access

Integrity
Ensuring Data Is Reliable and Accurate

Availability
Ensuring Data Is Available When Needed

Issue Spotting: Privacy Controls

People:

- Privacy Compliance Officer

Processes:

- Privacy Policy
- Information Security Policy
- Third-Party Data Processing Agreements, including Business Associate Agreements

Technology:

- Data Mapping

Issue Spotting: Security Controls

Written Information Security Program:

- Vulnerability Management
- Physical Access Restrictions (i.e., badging)
- Acceptable Use / Data Handling Policies
- Risk Assessments
- Incident Response Plan
- Security Training

Network Controls:

- Penetration Testing
- Network Segmentation
- Identity and Access Management (IAM)
- Multifactor Authentication
- Data Loss Prevention
- Encryption / Tokenization

MEDCON CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

U.S. Federal

FDA Guidance

- FDA has published guidance on cybersecurity, directed at medical device manufacturers.
  - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and FDA Staff
  - Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and FDA Staff
  - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software: Guidance for Industry
  - Best Practices for Communicating Cybersecurity Vulnerabilities to Patients

FDA Guidance

- Guidance: Postmarket Management of Cybersecurity in Medical Devices
- Exploitability risk can be “controlled” (acceptable residual risk) or “uncontrolled” (unacceptable residual risk).
- Controlled risk exploitability typically does not affect device’s safety or essential performance. Uncontrolled exploitability creates a potential safety threat and may affect essential performance.
- Manufacturers must report uncontrolled vulnerabilities to the FDA according to 21 CFR part 806, unless reported under 21 CFR parts 803 or 1004. However, the FDA does not intend to enforce reporting requirements under 21 CFR part 806 for specific vulnerabilities with uncontrolled risk when the following circumstances are met:

  (i) there are no serious adverse events reported

  (ii) manufacturer communicates with customers within 30 days, identifies compensating controls, and develops remediation plan to bring risk to an acceptable level

  (iii) manufacturer fixes the vulnerability ASAP and within 60 days

  (iv) manufacturer actively participates as a member of ISAO that shares vulnerability information and provides the ISAO with any customer communications upon notification of its customers

FDA Guidance

- FDA issued final guidance regarding “Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act” in March 2023
- FDA issued draft guidance regarding “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” in April of 2022
- This guidance furthers FDA’s continuing focus on cybersecurity, as illustrated by several notable actions in recent years, including reports and white papers including:
  - Playbook for Threat Modeling Medical Devices
  - Best Practices for Communicating Vulnerabilities to Patients
  - NIST Request on Presidential Executive Order
  - Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities

Federal Trade Commission

- Primary authority under Section 5 of the FTC Act
- May bring enforcement actions against organizations following data security incidents that FTC believes involve:
  - **Deceptive practices** – misrepresenting privacy and security measures
  - **Unfair practices** – inadequate security measures
- Has expressly stated its intent to further expand its role in setting and enforcing cybersecurity and data privacy standards

Federal Trade Commission

- **Health Breach Notification Rule**
  - September 15, 2021 Policy Statement broadly defines covered entities and breaches
  - Breach includes improper sharing (i.e., without users' authorization) of sensitive health information
- **"De Facto Breach Notification Rule"**
  - *"Regardless of whether a breach notification law applies, a breached entity that fails to disclose information to help parties mitigate reasonably foreseeable harm may violate Section 5 of the FTC Act."* - May 20, 2022 Blog Post

FTC Enforcement Activity

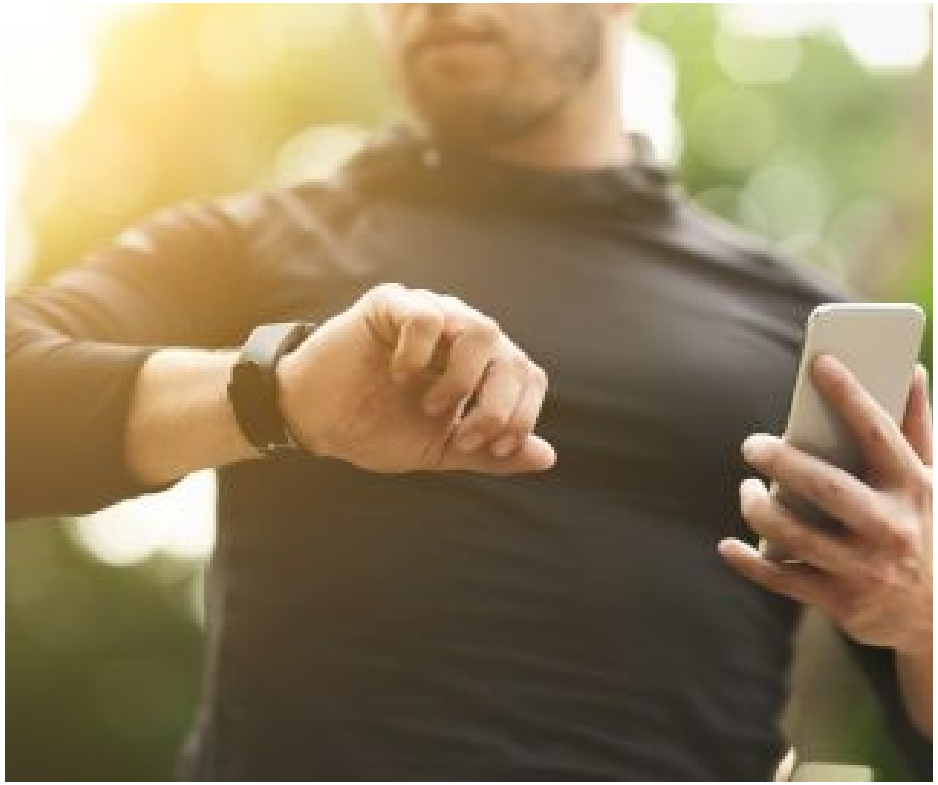
- Since 2020, life sciences companies and digital health applications received substantial FTC scrutiny
- Notable FTC enforcement activity included:
  - 2023 settlement with BetterHelp.
  - 2022 settlement with CafePress for covering up data breach and lax security.
  - 2021 settlement with mobile app Flo Health pertaining to its collection and use of health information.
  - 2020 settlements with Ortho-Clinical Diagnostics and Medable pertaining to misleading claims regarding participation in the EU-US Privacy Shield framework.
  - 2019 settlement with LabMD pertaining to security practices.

Cyber Threats – FTC

- FTC has signaled that cybersecurity will be an enforcement priority through recent settlements and announcements:
  - FTC's recent actions against Chegg and Drizly shows the FTC's continued focus on cybersecurity and potential consequences of failing to ensure adequate security
  - FTC warning to companies to remediate Log4j security vulnerability or face enforcement action illustrates FTC's intent to use legal authority to pursue companies that fail to protect consumer data against known security threats

FTC Enforcement Activity

- In 2021, FTC warned health applications and connected device companies to comply with the Heath Breach Notification Rule
- The Rule requires vendors of personal health records (PHRs) and related entities not covered by HIPAA
to notify individuals, the FTC, and sometimes the media of a breach of unsecured personally identifiable health data.
- The Rule applies to vendors of PHRs and any entity that (1) offers products or services through the web site of a vendor of PHRs; (2) offers products or services through the Web sites of HIPAA-covered entities that offer individuals PHRs; or (3) accesses information in a PHR or sends information to a PHR.
- In 2023, enforced the rule against GoodRx.



HHS – HIPAA Privacy Rule

- Limits the purposes for which PHI may be used and disclosed
- Establishes data subject rights

HHS – HIPAA Security Rule

- Requires appropriate administrative, physical, and technical safeguards
  - Flexible and scalable, but entities must continually review and modify
  - Required vs. Addressable specifications (e.g., risk analysis vs. termination procedures when employment ends)
- Examples of required administrative safeguards:
  - Risk analysis and risk management
  - Information system activity review
  - Security incident response and reporting system
  - Contingency planning (data backup, disaster recovery, emergency mode operations)

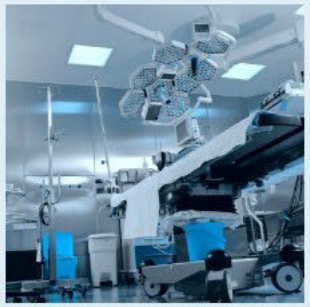
HHS – HIPAA Breach Notification Rule

- Requires covered entities to notify HHS, affected individuals, and potentially the media of any breach of unsecured protected health information.
- Notification must be provided without unreasonable delay and within 60 days of discovery.
- Notification to the media is required if more than 500 individuals are involved.

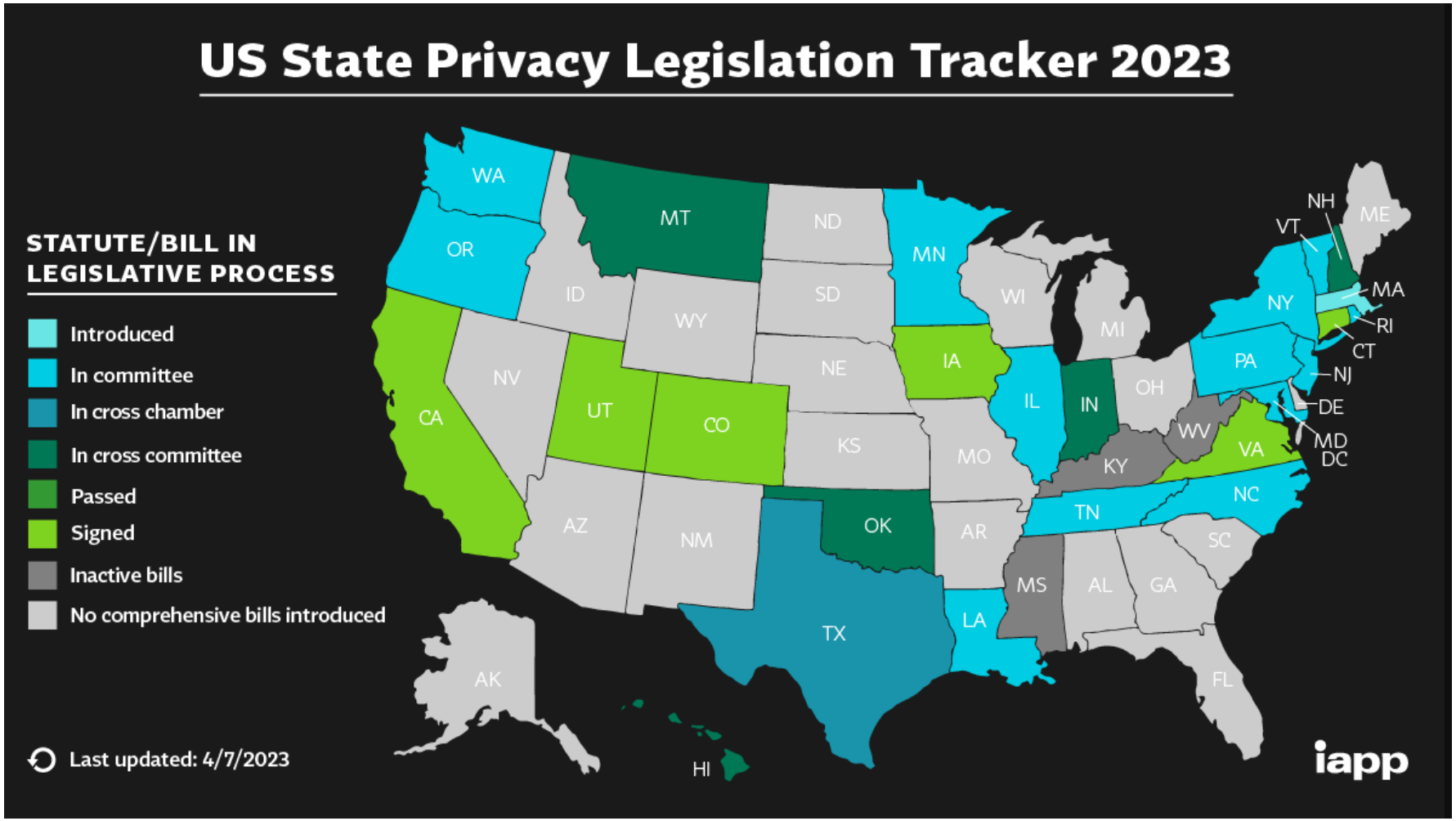
Strengthening American Cybersecurity Act

- Signed into law March 15, 2022
- Covers 16 Critical Infrastructure Sectors (including healthcare and public health and critical manufacturing)
- Unclear which companies within CI sectors are “covered entities”
- Final Rule must be issued by September 2025
- Requires covered entities to report to CISA within
  - 72 hours of discovery of a cybersecurity incident
  - 24 hours following any ransomware payments

U.S. State Laws



US State Laws



US State Laws

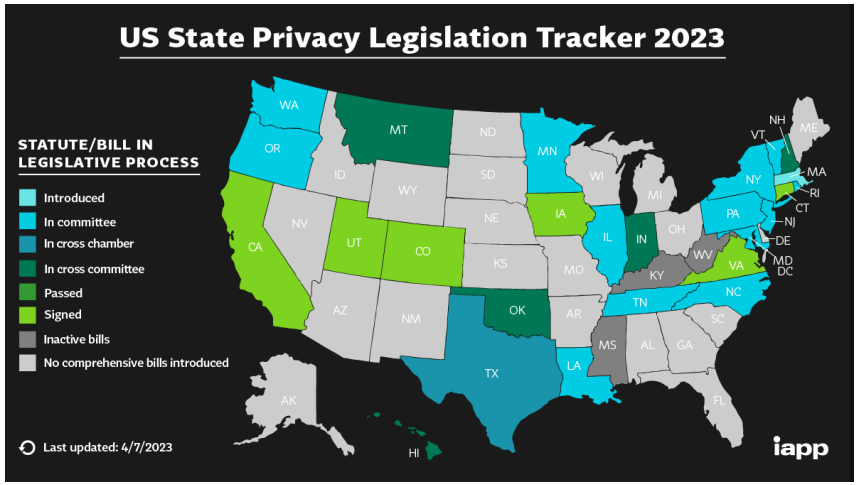
Applicability:

- All based on volume of information available to business
- California - $25m revenue threshold

Main requirements:

- Privacy policy
- Agreements with third parties
- Privacy impact assessments
- Reasonable security

Enforced by attorneys general



MEDCON CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

Issues for Device Manufacturers

Issues for Med Device Manufacturers

Cybersecurity

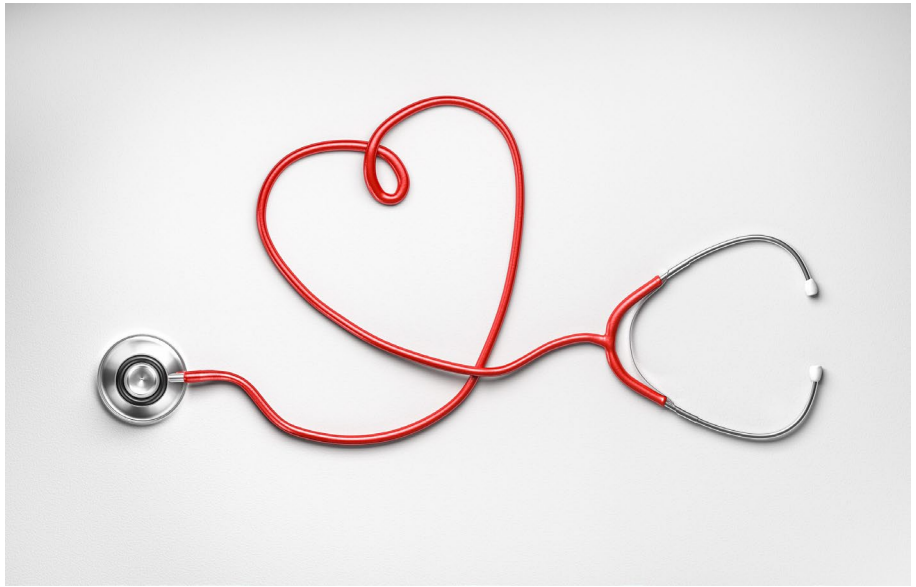
Connectivity

Collection of data from the user and healthcare providers

Automatic collection of data

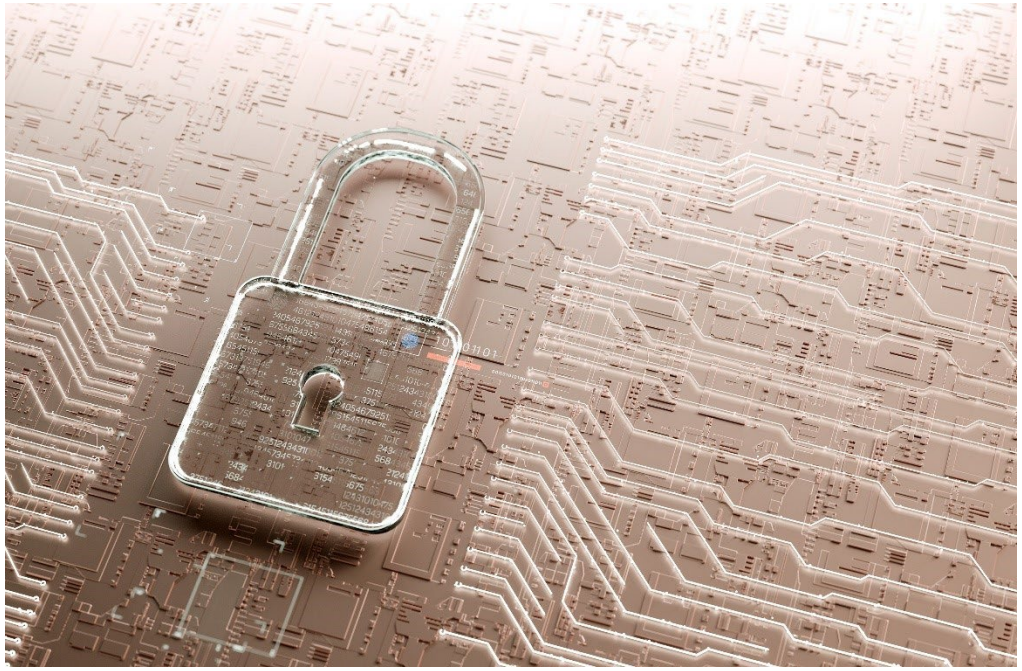
Residual data on devices

Full and timely disclosure of practices



Cyber Threats – Risks and Regulators

- Life sciences companies face numerous cyber threats in 2023, including:
  - Increasingly sophisticated cyber threats probing complex networks that include numerous third-party vendors and connected devices
  - Increased digitization requires prioritization of cybersecurity across the enterprise
  - Aging operational technology structures may lack adequate security
  - Remote and off-site workers accessing networks from potentially unsecured Wi-Fi
  - Complex and far-flung supply chains present a large attack surface
- Enforcement and regulation related to cyber threats will continue to involve a mosaic of federal regulators, including HHS-OCR, FDA, FTC, and others



MEDCON CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

GDPR and UK GDPR

GDPR & UK GDPR

- Applies when:
  - Legal entity present
  - Offering of goods or services
  - Monitoring of behavior
  - Citizenship of data subject not relevant
- Legal basis for processing: Consent, contract, legitimate interest, compliance with legal obligations
- Controller - Processor
- Pseudonymized – Anonymized Personal Data

GDPR & UK GDPR

- Medical devices:
  - Controller: customer contacts, employees, suppliers, clinical trial participants, users
  - Processor: customer patients/users, customer employees
  - Legal basis (controller): Legitimate interest, contract, consent, legal obligation
  - Information security
  - Cross-border transfers of personal data – transfer impact assessment
  - Monitoring of behavior – data protection officer
  - EU Member State requirements

GDPR & UK GDPR

- UK Data Reform
  - Broadens ability to use special category personal data for approved medical research by, for example, limiting need to reconsent data in certain circumstances
  - EU adequacy finding risk
  - Cross-border data transfers UK-US

GDPR & UK GDPR

- Data Privacy Framework ("Privacy Shield II"): Supplemental principles specifically address transfers of personal data from the EU to the U.S. in connection with medical devices
  - Adequacy finding still uncertain

GDPR & UK GDPR

- GDPR enforcement
  - (IT) medical app: health status of recipients disclosed in a campaign email with patient names on (cc), users required to accept both the contractual terms of use and the content of the privacy policy with a single 'click,' no ability to separately give consent to the individual processing operations, violation of the principles of fairness and transparency by providing users with confusing and sometimes erroneous information regarding the processing of personal data, failure to designate a representative in the EU as the contact person for all data protection issues.

MEDCON
CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

EU AI Act

EU AI Act

- Draft Regulation
- Significant debate re high risk, unacceptable risk AI Systems
- Draft Art. 23a imposes significant obligations on medical device manufacturers when:
  - The high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer;
  - The high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

EU AI Act

- Obligations relating to data and data governance:
  - Training, validation, and testing data sets must be subject to appropriate governance and management practices
  - Data must be relevant, representative, and to the best extent possible, free of errors and complete
  - State-of-the-art security and privacy-preserving measure

EU AI Act

- Quality management system
- Technical documentation
- Fines of up to 6% of global revenue

MEDCON CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

European Health Data Space

European Health Data Space

- Significant debate around interplay between other EU regulations such as GDPR
- Member State GDPR interpretations and varying EHR systems preventing EU access to health data
- Regulates primacy use and secondary use exchanges of health data

European Health Data Space

- Standardized EHR exchange format
- Member State digital health authority
- EU central platform for digital health
- Data holders must make electronic health data available for secondary uses – includes data generated by medical devices

European Health Data Space

- Broad range of secondary uses – research, development, innovation re medical devices, training, testing of algorithms for AI in medical devices
- Data permit
- Cross-border access for secondary uses - authorization