HIPAA PRIVACY & SECURITY

HEALTH APPS AND HIPAA BUSINESS ASSOCIATES RISING OBLIGATIONS IN PRIVACY AND HEALTH DATA

January 17, 2023

With You Today

ANDREW TOBEL
Director
Healthcare Industry Data Protection Leader

703-336-1522
atobel@bdo.com

JIM AMSLER
Director
Privacy in Technology Leader

615-493-5681
jamsler@bdo.com

Learning Objectives

- **Define the regulatory requirements** of Business Associates and Health Apps under the new privacy and health data rules.
- **Understand recent Online Tracking Technologies** (cookies, pixels, tags, etc.) guidance announced by OCR and how companies may respond.
- **Explore privacy regulatory guidelines** and their effects on Health Apps, including when not operating as a Business Associate.
- **Identify regulatory trends** from the U.S. Federal Trade Commission and U.S. Department of Health and Human Services, Office for Civil Rights, U.S. Securities and Exchange Commission and where enforcement actions may be headed.

Requirements of Business Associates and Health Apps

HIPAA Security, Privacy, and Breach Notification Rules

SECURITY RULE

Specifies that covered entities and their business associates must implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information (ePHI)

- **Administrative Controls:** risk analysis, access provisioning and review, workforce training, assessment of control efficacy
- **Physical Controls:** facility access and control, workstation and device security
- **Technical Controls:** Identity and access management, Audit capabilities, logging and alerting for data integrity, transmission security

Protects the Confidentiality, Integrity, and Availability of PHI

PRIVACY RULE

Sets standards for the use and disclosure of PHI

- Provides for appropriate safeguards to protect the privacy of PHI including the definition and authorized uses of de-identified PHI
- Limits and conditions on the uses and disclosures of PHI without patient authorization
- Sets forth patient rights over PHI, including rights to examine and obtain a copy of their health records, and to request corrections

Manages the Uses and Disclosures of PHI

BREACH NOTIFICATION RULE

Requires covered entities and their business associates to provide notification following a breach of unsecured PHI

- A breach is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI
- An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a Four Factor Risk Assessment
- Establishes the burden of proof by which Covered Entities and Business Associates must demonstrate that proper notification has been provided

Creates Requirements in Response to a Breach of PHI

Protected Health Information (PHI)

- If held by a covered entity or business associate, **Protected Health Information** (PHI) is information, including demographic data, in any media or form, that relates to:
  - the individual's **past, present or future** physical or mental health or condition,
  - the provision of health care to the individual, or
  - the **past, present, or future payment** for the provision of health care to the individual,
  - **and** that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).
- **Once PHI has been de-identified, it is no longer considered to be PHI.** De-identified PHI neither identifies nor provides a reasonable basis to identify an individual.

De-identification and PHI Identifiers

There are (only) two ways to de-identify PHI; either: (1) a formal determination by a qualified statistician; or (2) the removal of 18 specified identifiers:

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes;
3. All elements of dates (except year) for dates directly related to an individual, (including birth date, admission date, discharge date, date of death; and all ages over 89);
4. Telephone numbers;
5. Fax numbers;
6. Email address;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary number (Insurance ID);
10. Account number;
11. Certificate/license number;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. URLs;
15. IP Addresses;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code

Uses and Disclosures Overview

General Rules & Requirements

- A covered entity may disclose PHI to a business associate (BA) to create, receive, maintain, or transmit PHI on its behalf, if the covered entity obtains assurance that the BA will appropriately safeguard the information.
- A contract between the covered entity and business associate must establish the permitted and required uses and disclosures of PHI by the business associate.

Authorizations and Objections

- A covered entity may not use or disclose PHI without a valid authorization.
- A covered entity may use or disclose PHI, provided the individual is informed in advance of the use or disclosure.

Treatment, Payment, Operations (TPO)

- A covered entity may use or disclose PHI for its own treatment, payment, or health care operations.
- A covered entity may disclose PHI to another covered entity or health care provider for payment activities
- A covered entity may disclose PHI about an individual to other participants in the organized health care arrangement for any health care operations.

Specific Requirements and Use Cases

- De-identification/Re-identification
- Minimum Necessary
- Limited Data Set
- Fundraising
- Underwriting
- Verification

The “BA PLUS” Compliance Model

- **Business Associate Agreement or Business Associate Contract**
  - Required for all business associates.
  - Must contain elements specified at 45 CFR 164.504(e).
- **§ 164.502 and § 164.504 establishes** the permitted and required uses and disclosures of PHI by the business associate.

COVERED ENTITIES MUST ESTABLISH THAT THE BUSINESS ASSOCIATE WILL:

- Not use or further disclose information other than as permitted or required by the contract or as required by law,
- Use appropriate safeguards to protect electronic protected health information,
- Make available protected health information in certain circumstances required by covered entities,
- Make available protected health information for amendment and incorporate any amendments to protected health information,
- Provide records as appropriate to verify compliance with this rule.

Online Tracking Technologies Guidance

Office of Civil Rights (OCR)

Office of Civil Rights (OCR) has issued a bulletin on use of third-party cookies, pixels and other tracking technology by healthcare companies. The bulletin sets regulatory expectations for website and mobile app development for a wide range of companies subject to HIPAA, including hospitals, physician groups, health insurance plans, pharmacies, and other covered entities and business associates.

WHY WAS THE BULLETIN RECENTLY ISSUED?

Due to increase in number of class action lawsuits concerning healthcare companies and tracking technologies.

- Healthcare companies will need to perform a risk-assessment of their use of third-party tracking technology to determine if HIPAA requires them to send breach notifications.
- They need to work with their privacy and security departments to assess and mitigate ongoing risk as well as reassessing their strategy regarding third-party tracking.

OCR Regulatory Requirements For Online Tracking Technologies (OTT)

COMPLIANCE OBLIGATIONS WHEN USING TRACKING TECHNOLOGIES:

- Ensuring that all disclosures of PHI to tracking vendors are permitted by the Privacy Rule and that only the minimum necessary PHI to achieve the intended purpose is disclosed.
- Regulated entities should evaluate their relationships with tracking technology vendors to determine whether such vendor meets the definition of a business associate and ensure that the disclosures made to such vendors are permitted by the Privacy Rule. If there is a business associate relationship in place, the vendor must sign a Business Associate Agreement (BAA).
- Regulated entities must obtain an individual's HIPAA-compliant authorization before disclosing PHI to a vendor in situations where there is no business associate relationship in place. Privacy notices, website terms or website banners that ask users to accept or reject the website's use of cookies and other tracking technologies do not constitute a valid HIPAA authorization.
- A regulated entity's Risk Analysis and Risk Management processes under the Security Rule must address the use of tracking technologies.
- It is insufficient for a tracking vendor to agree to remove PHI from the data it receives or de-identify the PHI prior to the vendor storing the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA and that there is an application Privacy Rule permission for disclosure.
- The BAA must specify the vendor's permitted and required uses and disclosures of PHI, along with the safeguards for the PHI and must report any security incidents, including breaches of unsecured PHI.

Cookie, Banner, and Pixel Compliance

Cookie, Banner, and Pixel Compliance

Website compliance considerations are driven by applicable regulations, which requires understanding and documentation of:

- Business activities that collect, use, share, or otherwise process Personal Data or Personal Information
- Who is described by this Personal Data, where they live, and what regulations are imposed by the processing of their data
- Categories of information processed

Primer On Cookies

Cookies are text files stored on a client machine that may later be retrieved

- **First Party Cookies**
  Cookies placed by the website visited
- **Third Party Cookies**
  Cookies placed by a party other than the website visited (LinkedIn, Facebook, YouTube, etc.)
- **Session Cookie**
  Stored only as long as the browser is open
- **Persistent Cookie**
  Defined lifespan set by the developer. Users may only get rid of Persistent Cookies once the timespan elapses, or by expressly clearing them

European Privacy Laws and Online Profiles

Article 7 - Conditions for Consent

Controllers shall be able to demonstrate that they have obtained valid consent for all processing based on said consent, which:

- Must stand alone
- Be intelligible and easily accessible
- Use clear and plain language
- Must be able to be withdrawn as easily as given
- cannot be conditional if the processing is not necessary for a contract

Article 21 - Right to Object

When cookies are being used for direct marketing, the DS can object at any time, and at that point, the data should no longer be processed.

ePrivacy Directive

- Protection of privacy in the electronic communications sector
- Article 5(3) – consent must be obtained to store or access cookies on a user terminal
- Applies to all cookies except strictly necessary
- Purpose for processing must be presented clearly and comprehensively=> Cookie Banners

CCPA and Online Profiles

- CCPA does not implement cookie-specific requirements, but DOES enact requirements about what is being disclosed, and what is done with that data.
- Identifiable information collected by cookies is considered personal data.
- Cookie-derived data is afforded the same rights and protections as any other Personal Information.
- CCPA consent model is Opt-In.
- CCPA requires disclosure of data being collected by cookies, and what (specifically) is done with that data.
- Opt-Out of the “Sale” of Personal Information **MUST** be applied to Cookie Data.

Implementing Consent Models

- Geolocation Rules infer user location and apply appropriate Consent Models
- GDPR and LGPD implement opt-in
  - Implementation:
    - Place only place strictly necessary Cookies
    - Users Opt-In to all other types
- Implied consent means navigating the website = consent
  - Not valid under the GDPR!
- CCPA implements Opt-Out
  - Implementation:
    - Place all cookies on the machine
    - Do not access Cookies upon Opt-Out

Path to Compliance

Privacy Contact Requirements

The identity and contact details of the organization, its representative, and its Data Protection Officer

> *If you have any questions about Our Company's privacy policy, the data we hold on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact us.*
>
> *Should you wish to report a complaint or if you feel that Our Company has not addressed your concern in a satisfactory manner, you may contact the…* (Regulatory Authority)

One or more designated means for consumers to submit requests, including (at minimum) a toll-free number.

Other examples:

- Privacy Mailbox (privacy@company.com)
- Web-based inquiry form
- Mailing address

Compliance Actions (1)

Regardless of regulatory obligations, companies should consider the following steps as they institute compliance measures on websites, applications, and other corporate data collection points:

- Creating/updating a privacy-related webpage that includes clear and conspicuous contact details
- Drafting a Privacy Notice that, at a minimum, answers the following:
  - Who are you?
  - What information are you collecting?
  - How are you going to use the information?
  - With whom will you share the information?

Compliance Actions (2)

Regardless of regulatory obligations, companies should consider the following steps as they institute compliance measures on websites, applications, and other corporate data collection points:

- Drafting a Personal Data Inventory that documents the Personal Data your organization collects, the individuals described by this data, and how the data is processed and shared
- Reviewing and being ready to provide proof of the successful implementation of cookies and tracking technologies
- Updating the Privacy Notice to reflect the Personal Data Inventory (potentially iterative)
- Implementing Consent models that correspond to the obligations applicable to your organization's scope and processing

Compliance Actions (3)

Regardless of regulatory obligations, companies should consider the following steps as they institute compliance measures on websites, applications, and other corporate data collection points:

- Instituting processes and controls that support the validation, orchestration, and fulfillment of Individual Rights Processes
- Where required, evaluating and implementing appropriate technology platforms and controls that automate and / or implement required processes
- Instituting periodic assessments and reviews to update the Personal Data Inventory, Notice, Consent, and corresponding process and technology supports that support compliance

Regulatory Trends and Enforcement Actions

U.S. Department of Health and Human Services

The current Notice of Proposed Rulemaking (NPRM) by HHS will improve care coordination, ease patient privacy concerns, and break down barriers to information sharing by easing compliance complexities and providing patients with additional rights.

CURRENT STATE

These requirements create the following:

- Barriers to information sharing by patients and amongst health care providers.
- Dual obligations and compliance challenges for regulated entities.

Confidentiality of Substance Use Disorder Patient Records regulations, commonly called 42 **CFR Part 2** imposes different requirements with Substance Use Disorders (SUD) treatment records than the HIPAA Privacy Rule.

PROPOSED CHANGES

- Permitted use and disclosure of Part 2 records based on a single patient consent given once for all future uses and disclosures for treatment, payment, and health care operations.
- Permitted redisclosure of Part 2 records in any manner permitted by the HIPAA Privacy Rule, with certain exceptions.
- New patient rights under Part 2 to obtain an accounting of disclosures and to request restrictions on certain disclosures, as also granted by the HIPAA Privacy Rule.
- New HHS enforcement authority, including the imposition of civil money penalties for violations of Part 2.
- Updated breach notification requirements to HHS and affected patients.
- Updated HIPAA Privacy Rule Notice of Privacy Practices requirements to address uses and disclosures of Part 2 records and individual rights with respect to those records.

Part 2 only applies to Substance Use Disorders (SUD) treatment records

Additional Trends

Securities and Exchange Commission (SEC)

New proposed rule would require the following:

- Cyber incident reporting
- Four days to report material incident
- Cyber risk management and strategy
- Cyber governance

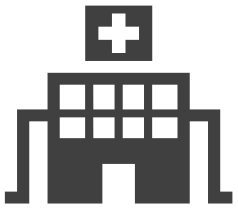
Federal Trade Commission (FTC)

- FTC issued Advanced Notice of Proposed Rule (ANPR) making on commercial surveillance and data security
  - Currently, the FTC wants to generate a public record. Based on this public record, it will consider regulatory approaches
- This could be the beginning of a push by the FTC on a comprehensive data privacy and security law regime

Health Apps Privacy Regulation Guidelines

Regulatory Requirements of Health Apps

A HEALTH APP MUST MEET HIPAA COMPLIANCE REQUIREMENTS:



If it is used by the **covered entity or business associate**

If it **accesses, produces, or stores protected health information (PHI)**

The FTC Act: Data collected by health apps is regulated by the Federal Trade Commission (FTC) under the Health Breach Notification Rule, which applies to all non-HIPAA regulated entities that maintain a consumer's "personal health record."

Federal Drug and Cosmetics (FD&C) Act: The FDA enforces the FD&C Act, which regulates the safety and effectiveness of medical devices and mobile medical apps.

Federal Laws and Regulations for Mobile Apps

HIPAA Privacy, Security and Breach Notification

- These Rules apply to covered entities or their business associates that create, receive, maintain, or transmit protected health information.
- Those creating health apps or offering health apps on behalf of covered entities may be considered business associates of covered entities, thus requiring those health apps to abide by the HIPAA Rules.

Federal Trade Commission Act (FTC Act)

- Even if the protected health information is not protected by the HIPAA Rules, there is still a federal law requirement that health apps would be obligated to abide by, known as the FTC Act.
- The FTC Act applies to most app developers and expects them to adopt and maintain reasonable data security practices, such as minimization of data, limiting access and permissions, implementing security by design, etc.

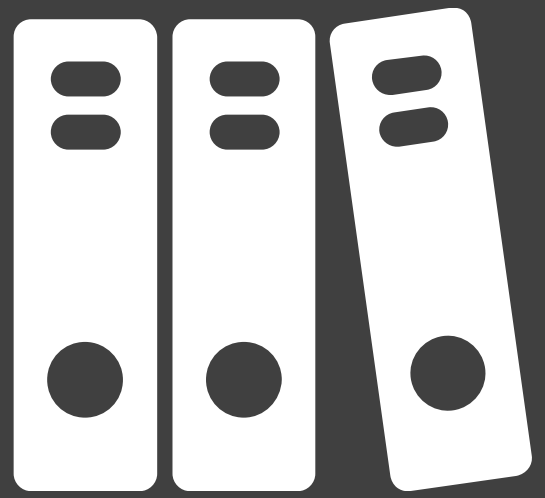
Federal Food, Drug, and Cosmetic Act (FD&C Act)

- The FD&C Act considers a software function to be a medical device and subject to FDA device regulation if meeting definition of device in section 201(h) of the FD&C ACT i.e. When a software function is intended for use in the diagnosis of disease or other conditions, thus health apps or medical apps intended for use would fall under this Act's requirements.

The HHS Office of the National Coordination for Health Information Technology (ONC)

- Prohibits information blocking by health care providers, health IT developers of certified health IT, or health information network. Information blocking refers to practices that would interfere with access, exchange, or use of electronic health information.

Appendix



Helpful Resources for Health Apps

Mobile Health App Interactive Tool	▶ Developed by FTC in conjunction with OCR, HHS, ONC, and the FDA ▶ Interactive tool to help users understand laws and rules that may apply to health apps ▶ Developed for anyone developing a mobile app that will access, collect, share, use, or maintain information related to an individual consumer's health
Health App Use Scenarios & HIPAA (HHS)	▶ PDF guide detailing various scenarios for health applications.
Access Right, Apps, and APIs (HHS)	▶ Frequently asked questions about how HIPAA rules apply to covered entities and their business associates
Health Information Technology (HHS)	▶ Frequently asked questions on HIPAA and health IT
Guidance on HIPAA & Cloud Computing (HHS)	▶ OCR developed guidance to assist cloud service providers in understanding HIPAA obligations for cloud computing technologies.

About BDO USA

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

www.bdo.com