ACC Life Sciences Conference – Applying Traditional Health Regulations to the Fast-Evolving World of Digital Health

Paul Pitts, James Hennessy, and Tori Lallemont
May 10, 2023

ReedSmith
Driving progress
through partnership

What is Digital Health?

A broad term denoting health care's digital transformation.

Represents technological advancements changing existing health care infrastructure and creating new opportunities for innovation, access, and equity.

Includes:

- Health information technology
- Electronic health records ("EHR")
- Digital health applications
- Health data analytics and informatics
- Telehealth

Digital Health in Practice

For health care providers, companies, or patients:

Technology to support, manage, and increase access to health information or services, including:

- Telehealth platforms, EHR, health IT software, AI, SaMD

For consumers:

Technology providing opportunities to participate in a consumer's own health and wellness, including:

- Web-based or mobile apps, wearable devices

Digital Health Practical Example: **Telehealth**

Health care services delivery via electronic telecommunication platforms, including:

- Virtual patient visits, remote patient monitoring, virtual medical imaging, asynchronous patient-provider messaging

Expands health care services access and increases availability in underserved and rural areas.

- COVID-19 pandemic accelerated need for alternatives to in-person health care services delivery.

Surge in utilization and access has invited regulatory scrutiny and enforcement.

Fraud and Abuse in Health Care

Health care fraud: Intentional deception or factual misrepresentation that may result in unauthorized benefit or payment for health care services.

Health care abuse: improper, inappropriate, or unacceptable activities that fall outside standards of professional conduct or are medically unnecessary.

Underlying Fraud and Abuse Principles

1. Treatment should be based on clinical decision making and the best interests of the patient (not commercial interests)
2. Unnecessary referrals are costly to federal health care programs and may result in unfair competition
3. Access to health information should be limited to the minimum amount necessary outside of legitimate treatment activities
4. Provider and patient users presume health IT alerts/messages to be driven by objective, clinical information (not marketing)
5. Widespread use of interoperable digital health technologies benefit patients but these technologies may have significant independent value

Suspect Activities and Arrangements

- Kickbacks
- Up-coding time and complexity
- Misrepresenting the virtual service provided
- Submitting claims for services not medically necessary
- Billing for services not rendered
- Unbundling
- Falsifying government health care program participation eligibility

Fraud and Abuse Legal Frameworks

1. **Anti-Kickback Statute ("AKS")**
2. **False Claims Act ("FCA")**
3. **Stark Law**
4. **State corporate practice of medicine prohibitions**
5. **State fee-splitting laws**
6. **Beneficiary inducement laws**
7. **Health Insurance Portability and Accountability Act of 1996 ("HIPAA")**
8. **Insurance and Medicare/Medicaid coverage requirements**

Fraud and Abuse Legal Frameworks – Anti-Kickback Statute ("AKS")

Federal criminal statute (42. U.S.C. § 1320a07b(b)) prohibiting paying, offering, soliciting or receiving remuneration to induce another individual to purchase or refer health care services reimbursable by a federal health care program.

"Remuneration" broadly defined to mean anything of value, including cash, free or discounted services, waivers of co-pays or deductibles, payments or other business opportunities that are not FMV or commercially reasonable

Scienter requirement: violation requires acting knowingly or willfully

Penalties include: imprisonment, criminal monetary fines, exclusion from Medicare/Medicaid

Fraud and Abuse Legal Frameworks – False Claims Act ("FCA")

Federal civil and criminal statute (18 U.S.C. § 1347) prohibiting any person or corporation from knowingly submitting a false or fraudulent claim for payment to the federal government.

Authorizes qui tam or "whistleblower" suits allowing private individuals or corporations to file actions alleging evidence of fraud against the federal government.

Penalties include: repayment of false claim, civil monetary fines, exclusion from Medicare/Medicaid

Many states have parallel false claims prohibitions.

Fraud and Abuse Legal Frameworks – Stark Law

Federal Physician Self-Referral Law (42 U.S.C § 1395nn) prohibits physicians from referring "designated health services" reimbursable by Medicare to entities with which the physician (or an immediate family member) has a financial relationship.

"Designated health services" include clinical laboratory services, radiology and imaging services, physical therapy, occupational therapy, radiation therapy, home health services, outpatient Rx drugs, inpatient and outpatient hospital services, durable medical equipment and supplies.

Stark Law applies unless the referral or arrangement qualifies for a specific exception.

Penalties include: repayment or no payment for improper referral, civil monetary fines

Fraud and Abuse Legal Frameworks – HIPAA

Federal law and regulatory scheme designed to prevent unauthorized disclosure of protected health information ("PHI").

Does not apply to health information broadly, only to "covered entities" (i.e., most health plans, clearinghouses, and providers) and their business associates.

Permissible PHI uses and disclosure include:

- Legitimate treatment, payment, and health care operations
- Patient safety and public health
- Marketing or sale of PHI but only upon obtaining individual authorization

States and the federal government also have parallel privacy laws, breach notification laws, and consumer protection laws (e.g., TCPA, CAN-SPAM, COPPA, CCPA, CPRA)

Fraud and Abuse Legal Frameworks – CPOM

Federal law and regulatory scheme designed to prevent unauthorized disclosure of protected health information ("PHI").

Designed to protect clinical and professional judgment from improper corporate influence.

No general federal prohibition:

- States with strong CPOM prohibitions: California, New York, Texas, Washington State
- States with no or unenforced CPOM prohibitions: Alaska, Florida, Utah, Virginia

Common CPOM solution involves forming a management services organization (MSO) to manage a health care practice's non-clinical operations.

- Failure to properly form management arrangement may result in invalidation of agreement and other penalties

Fraud and Abuse Legal Frameworks – Beneficiary Inducement Laws

Prohibits health care providers and suppliers from offering inducements to Medicare and Medicaid beneficiaries that are likely to influence their decision to receive health care items or services from a particular provider or supplier.

Aims to ensure beneficiaries make health care decisions based on medical need rather than financial incentives.

Violations may result in significant financial penalties.

Potential Penalties

Anti-Kickback Statute (AKS)

Up to 5 years in prison, up to $104,000 per violation, plus 3x the amount of remuneration; mandatory exclusion from federal health care programs; collateral consequences include FCA liability

False Claims Act (FCA)

Treble damages + $20,000 per claim, plus criminal penalties (imprisonment, criminal fines).

Stark

Repayment of improperly received federal health care program funds, civil monetary fines, potential FCA liability.

CPOM

Potential criminal liability; loss of licensure; financial penalties; invalidation of agreements.

HIPAA

Enforcement CMP levels from $100 to $60,000 per violation, potential criminal liability

Digital Health Trends and Enforcement Actions

Fraud and Abuse Enforcement Trends: Telehealth

Reasons for historically less telehealth enforcement:

- lower volume of services
- lack of coverage and payment by third-parties
- absence of referral relationships

Increase in use of telehealth during the COVID-19 pandemic resulting in increased false claims cases, including:

- Non-covered services (e.g. unauthorized originating sites, unqualified practitioner, unallowable means of communication)
- Kickbacks
- Unnecessary prescriptions, lab tests, or medical devices
- Incorrect codes (e.g. codes requiring in-person service)

COVID-19's Telehealth Regulatory Impact

To minimize pandemic's public health impact, state and federal regulators implemented temporary regulatory flexibilities to expand health care access, including:

- **OIG issued policy statement permitting practitioners to reduce or waive cost-sharing obligations, including coinsurance and deductibles, for telehealth services paid for by federal healthcare programs**
- **CMS relaxed or suspended Medicare rules for supervisory of telehealth services**
- **CMS increased telehealth modalities for patient-provider visits and list of telehealth services reimbursable by Medicare**
- **CMS implemented Stark law waivers**
- **Elimination of prior provider-patient relationship requirements**
- **OCR relaxed HIPAA enforcement and requirements, allowing use of various non-public facing platforms for telehealth (e.g., Facetime, Skype, Zoom, etc.) and exercising enforcement discretion for good faith use of telehealth**

States broadly took similar steps in the immediate wake of the pandemic

COVID-19 Induced Telehealth Surge

Aided by relaxed regulatory environment, Telehealth usage surged:

- According to CMS, nearly half of Medicare primary care visits conducted via telehealth in April 2020, compared to 0.1% in February 2020
- According to HHS, Medicare visits conducted via telehealth in 2020 increased *63-fold*, from 840,000 in 2019 to 52.7m in 2020
- Global telehealth market predicted to reach $113b by 2025 (valued at ~$25b in 2016).

Telehealth Trends to Watch

- Increased expenditure on all types of telehealth services.
- Medicare coverage expansion.
- New state legislation promoting parity.
- More audits, investigations, enforcement actions, and payor disputes.
- Greater integration of telehealth services with labs, pharmacies, specialists, and ancillary services.
- Rising privacy concerns and scrutiny over breaches.

Recent Digital Health Enforcement Actions: Digital Pharmacies

Truepill: December 2022

- DEA alleged digital pharmacy company unlawfully dispensed thousands of controlled substances (e.g. over-prescribing, improper clinician licensure, etc.)
- Now being investigated by DOJ for its prescribing practices under the Controlled Substances Act.

Pill Club: February 2023

- Online women's pharmacy reached $18.3m settlement with CA for alleged Medi-Cal fraud
- CA Attorney General claims company defrauded Medi-Cal program by prescribing certain contraceptives without adequate consultation, billing Medi-Cal for those contraceptives.
- Whistleblower complaint alleges as little as 15 seconds spent on visits prior to prescribing.

Recent Digital Health Enforcement Actions: Electronic Health Records

Athenahealth: January 2021

- Health care technology company paid $18.25m to resolve allegations that it paid kickbacks to generate EHR product sales
- Kickbacks may have caused health care providers to submit false claims for incentive payments for achieving Meaningful Use

EHR Software Company: April 2021

- Company resolved allegations that its marketing referral program violated the FCA and AKS by providing clients cash equivalent credits, cash bonuses, and percentage success payments to recommend its products

Modernizing Medicine ("ModMed"): November 2022

- Technology vendor fined $45m for alleged violation of FCA by accepting and providing unlawful remuneration in exchange for referrals by causing its users to report inaccurate information for federal incentive payments

Recent Digital Health Enforcement Actions

DOJ Telefraud Takedowns

- Operation Brace Yourself (April 2019): focused on a number of alleged kickback schemes relating to DME prescriptions, totaling over $1.2b in losses

- Operation Double Helix (September 2019): focused on alleged kickback schemes where physicians paid to order genetic testing without any patient interaction or after limited consultation, totaling over $2.1b in losses

- Operation Rubber Stamp (October 2020): charged companies and individuals with alleged kickback schemes relating to improper DME prescriptions and orders for medically unnecessary genetic testing, totaling over $1.5b in losses

Recent Digital Health Enforcement Actions

Sept. 2021: U.S. DOJ announced criminal charges against 138 defendants, including 42 licensed health care professionals, across 31 federal districts for participation in a $1.1b fraudulent telehealth scheme.

- Connected to substance abuse treatment facilities.
- Prescribers allegedly paid to order medically unnecessary DME, genetic and other diagnostic testing, and pain medications without having any meaningful interaction with patients.

July 2022: DOJ announced charges against 36 defendants, including licensed health care professionals, across 13 federal districts for participation in $1.2b fraudulent telehealth scheme related to cardiovascular and cancer genetic testing and DME.

HHS-OIG July 2022 Special Fraud Alert

U.S. OIG published a Special Fraud Alert in July 2022 highlighting "suspect" telemedicine arrangements.

Detailed key findings from OIG's various investigations into fraudulent schemes involving companies that provide telehealth, telemedicine, and telemarketing services.

OIG highlighted seven "suspect" characteristics commonly associated with fraudulent arrangements.

Alert issued to highlight recent enforcement and OIG's increasing scrutiny of telehealth arrangements.

HHS-OIG July 2022 Special Fraud Alert – "Suspect" Arrangements

1. Patients identified or recruited by telemedicine company (or another third party) and/or via advertising campaigns offering free or low-cost services.

Often present in "closed loop" arrangements where company markets items/services and patient is then directed to participating providers who make referrals for those items/services.

2. Treating practitioner does not have meaningful patient contact or information to make valid medical necessity assessment.

Interactions often brief, limited, and made through the use of audio-only technology.

HHS-OIG July 2022 Special Fraud Alert – "Suspect" Arrangements

3. Practitioner paid based on the volume of items or services ordered or prescribed or the number of medical records reviewed.

Potential to inappropriately influence decision-making and incentivize compensation.

4. Items or services only offered to federal health care plan beneficiaries.

Could result in coercive practices involving vulnerable patient populations.

5. Items or services only offered to individuals who are not federal health care plan beneficiaries, but which may ultimately result in inappropriate billing to federal health care plans for related items or services.

May not protect beneficiaries from related services that are part of larger arrangement.

HHS-OIG July 2022 Special Fraud Alert – "Suspect" Arrangements

6. Provision of only one product or service, restricting a practitioner's professional decision-making to a pre-determined course of treatment.

May also be present in "closed loop" referral arrangements described in #1.

7. No practitioner follow-up with patients receiving the items or services offered (e.g., no discussion of genetic testing results between patient and practitioner).

Limited practitioner involvement and oversight over a patient's care raise questions about the validity of that patient-practitioner relationship.

Expanded Theories of Fraud and Abuse Liability

What is reimbursable by a federal health care program?

- Must determine whether use of health IT, such as enhanced EHR functionalities and digital practice management tools, falls within recognized safe harbors or exceptions.

What health IT/data have strong potential for misuse?

- Using PHI without authorization for commercial gain can result in conspiracy to commit fraud under HIPAA.
- EHR data can be used in connection with kickback schemes to promote commercial interests, such as a fraudulent scheme to increase opioid prescriptions prosecuted in Jan. 2020.

What constitutes "white coat marketing" in the age of digital health?

- Using PHI without authorization for commercial gain?

Tools for Supporting your Company and Patients/Clients

Fraud and Abuse Compliance Myth-Busting

I don’t need to worry about or invest in compliance because:

- I’ve carved out federal health care program business.
- I’m not the type of bad actor regulators have targeted thus far.
- I’ll get around to it later.
- There has not been any enforcement activity in my particular space.
- The company is too small/early-stage to worry about this.

Digital Health Key Considerations

When offering or sponsoring health IT tools, resources, and functionalities to health care providers or patients, assess the following:

1. **Who is the intended user?**
2. **What is the purpose of the digital health tool?**
3. **Will the government be asked to pay for a good or service informed by its use?**
4. **Is the tool branded or unbranded? Are sales and marketing involved?**
5. **What is existing or desired commercialization strategy?**

Safeguards to Prevent Digital Health Fraud and Abuse

When offering or sponsoring health IT tools, resources, and functionalities to health care providers or patients, consider implementing the following

Questions?

Paul Pitts | Partner
+1 415 659 5971
ppitts@reedsmith.com

James Hennessy | Partner
+1 415 659 5962
jhennessy@reedsmith.com

Tori Lallemont, VP, AGC
One Medical
tlallemont@onemedical.com