Post & Schell PC
ATTORNEYS AT LAW

Privacy and Portals: Progress or Peril?

Mark L. Mattioli

October 2, 2025

www.postschell.com

1

Objectives

- Understanding and Avoiding Latest OCR Enforcement Efforts
- Recognizing "Information Blocking"
- Potential Issues Arising From Patient Portals

2

It All Starts with HIPAA

- Privacy
- Security
- Breach
- Enforcement

Some Basics

- Who is a Covered Entity?
- What is a Business Associate?
- Treatment, Payment and Health Care Operations?

It All Starts with HIPAA

- Office for Civil Rights (OCR) Enforces
  - Civil Fines:
    - Lack of Knowledge - $35,581
    - Reasonable Cause - $71,162
    - Willful Neglect (corrected) - $71,162
    - Willful Neglect (uncorrected) - $2,134,831
    - Maximum Annual - $2,134,831

5

Most Investigated Issues

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2021	Impermissible Uses & Disclosures	Access	Safeguards	Administrative Safeguards	Breach - Notice to Individual
2020	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Technical Safegards
2019	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2018	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safegards

6

Trends

- Ransomware
- Risk Analysis
- Right to Access Information
- Business Associate
- New Audits

7

Ransomware Cases

- Twelve Cases to Date
- Comprehensive Neurology PC
  - IT network encrypted – 6,8000 Individuals
  - $25,000 Fine and CAP
    - Single Doctor with only 5 employees
- Guam Memorial Hospital
  - 5,000 individuals
  - $25,000 Fina and CAP

8

Risk of Faulty Risk Analysis

- Eight Cases To Date
- Northeast Radiology
  - $350,000 for access to radiology images
- Health Fitness Corp.
  - Business Associate
  - $227,816 for software misconfiguration

9

Right of Access

- So far 53 actions based on Right of Access
- Gums Dental Care
  - $70,000 fine against solo dentist
  - OCR sent letter to gain compliance
- Rio Hondo Community Medical Center
  - $10,000 Fine

10

Business Associates

- Solara Medical Supplies
  - $3,000,000 resolution – incorrect addresses
- USR Holdings
  - $337,750 – Unauthorized Access
- Virtual Private Network
  - $90,000 – Ransomware incident
- Elgon Information Systems
  - $80,000 – Ransomware incident

Audits

- Focus on response to cyberattacks and ransomware
  - Risk Analysis
  - Backup and Recovery
  - Audit and Authentication
  - Training
  - Incident Procedures

Audits (cont'd)

- 50 Voluntary Audits
- Supposedly No Enforcement
  - But could result in Additional Review

Post&Schell PC ATTORNEYS AT LAW

13

Tracking Technology

- Question of Whether Tracking Technologies on Unauthorized Sites are Subject to HIPAA
  - Authorized = Patient Portals and Logins
  - OCR concerned with unauthenticated general information webpages
- Am. Hosp. Ass'n v. Becerra, 738 F.Supp.3d 780 (N.D. Tex. 2024)
  - Vacating Guidance for unauthorized websites

Post&Schell PC ATTORNEYS AT LAW

14

SNF Breaches

- Aloha Nursing - 20,016 patients – Unauthorized computer access
- Williamsport Home – Cyber attack
- Majestic Care – Unauthorized Access
- Virtual Care Provider Inc. – $14M ransomware attack affecting 100 SNFs
- Catholic Health Care Services – $650,000 fine of BA
- Hillcrest Nursing – $55k fine for lack of access

Reproductive Rights

- Purl v. United States Dept. Health & Hum. Serv., No. 2:24-cv-0288 (N.D. Tx., June 18 2025)
  - Vacated on National Level HIPAA Amendments in response to Dobbs
    - Argued they impinged state laws
    - Exceeded Statutory Authority under "Major Question Doctrine."

21st Century Cures Act

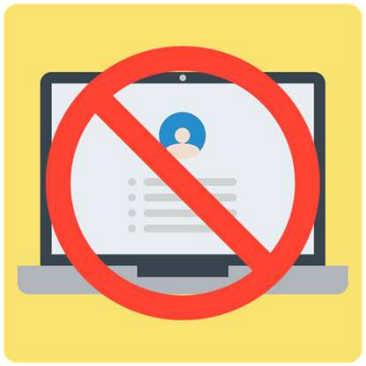
- Designed to promote "Interoperability" of Health Care Data
  - Alleviate administrative burdens to start of clinical trials
  - Enhance data sharing among NIH-supported researchers
  - Improve privacy protections for research volunteers

Empowering Patients and Improving Patient Access to Electronic Health Records

- The National Coordinator and the Office for Civil Rights of the Department of Health and Human Services shall jointly promote patient access to health information in a manner that would ensure that such information is available in a form convenient for the patient, in a reasonable manner, without burdening the health care provider involved.

Information Blocking

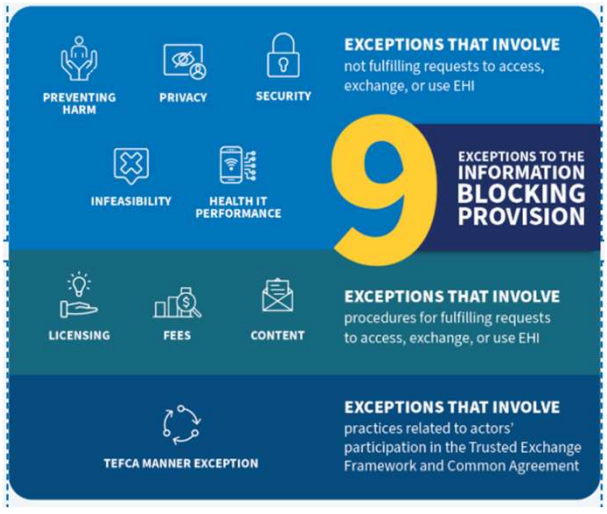
- Information blocking means a practice that except as required by law or covered by an exception set forth in subparts B, C, or D of this part, is likely to interfere with access, exchange, or use of electronic health information



Post&Schell PC
ATTORNEYS AT LAW

19

Information Blocking (cont'd)



Post&Schell PC
ATTORNEYS AT LAW

20

Exceptions

- Preventing Harm – substantial reduce harm to patient or other person
- Privacy Exception – comply with state or federal requirements
- Security Exception – safeguarding information
- Infeasibility – can't do

21

Exceptions (cont'd)

- IT Performance – interfere with access, exchange or use of electronic health information
- Protecting Care Access – reduce potential exposure to legal action

22

Exceptions – Fulfilling Request to Access

- Manner Exception – Technically Unable
- Fees Exception – Reasonable Fees
- Licensing Exception – Reasonable Royalty

Post&Schell PC
ATTORNEYS AT LAW

Exceptions – Participation in Exchange TEFCA Framework

- Trusted Exchange Framework and Common Agreement (TEFCA)

Post&Schell PC
ATTORNEYS AT LAW

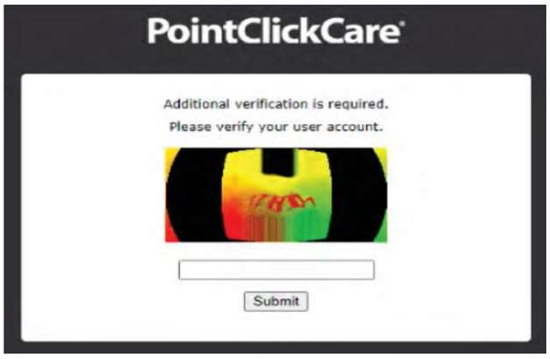
Real Time Medical Sys., Inc. v. Pointclickcare Tech., Inc.

- Alleged Blocking by Defendant
  - Software reviewed medical records
  - Claimed Bots caused performance concerns
  - Pointclick began using CAPTCHAs to stop automated access

Post&Schell PC ATTORNEYS AT LAW

Pointclick (cont'd)

- New "Unsolvable" CAPTCHA



Post&Schell PC ATTORNEYS AT LAW

Pointclick (cont'd)

- Use of Cures Act as Foundation for Unfair Trade Claim
  - No Private Cause of Action Under Cures Act
  - Enforced by Secretary of HHS
    - $1,000,000 per violation

27

Patient Portals

- Applies to Electronic Records
- No Actual Reequipment for a Portal
  - Right of Access under HIPAA
    - Information Blocking under Cures
- ONC – Suggested Use of Portal

28

Portals (cont'd)

- Ramifications
  - Access
  - How Much Information Should be Available?
  - Who Should Have Access
  - Risk of Breach
    - Deer Oaks – The Behavioral Health Solution
      - $225,000 Fine related to Patient Portal
      - Data for 171,871 individuals on Dark Web

Questions?

Mark L. Mattioli

Co-Chair, Health Care Practice Group
Post & Schell, P.C.
215-587-1113
mmattioli@postschell.com