

BIPA/Social Media and Privacy: Managing Provider Liability Arising From Technology

1

Website Tracking

- Many websites utilize apps and tools to collect, analyze, or share **website input and activity** by website visitors.
- A new wave of **web tracking lawsuits** impact companies using these tools to collect their website visitors' data.



2

OCR's Take on Website Tracking

"Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosure of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

3

Targeted Tools

**Session Replay
Software**

Chatbots

4

Session Replay Software

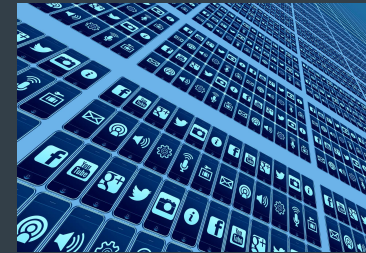
- Designed to **capture information at regular intervals** to allow the consumer's interface to be recreated.
- Records **mouse clicks, keyboard strokes, zooming, or cursor movements**.
- Intended to **assist with consumer experience, compliance, and website operations**.



5

Chatbots

- Engage users** and help **find desired content** on a website.
- Intended to be **cost-efficient tools** allowing companies to communicate with consumers in real time.
- Recording these conversations can **identify areas of consumer confusion or create better automated chatbot options**.



6

Types of Claims

Federal Wiretap Act	State Anti-Wiretapping Laws	Video Privacy Protection Act	"Intrusion Upon Seclusion"
Negligent Misrepresentation	Invasion of Privacy	Breach of Contract	Breach of Fiduciary Duty

7

Steps you should take

- Restrict the use of tracking technologies
- De-identify the data such that it falls outside the scope of the definition of PHI.
- To the extent that PHI exists online, it should arguably be secured by authentication and shielded from impermissible use or disclosure.
- "Sever" identifying information (such as session tokens, IP addresses, geolocation hop data, and similar) from tracking technologies, particularly where these technologies are critical for the functionality of the platform.
- Enter into business associate agreements governing the use and disclosure of PHI with third-parties that provide services online or confirming the HIPAA authorization of individuals before PHI is shared with these parties.

8

Let's Get Social



Nursing Homes get in hot water

- Nursing home employees' social media use cause big problems with:
 - HIPAA/privacy violations
 - CMS/State survey deficiencies and enforcement
 - Criminal charges against offending employees
 - News reports about offensive actions at nursing home

Privacy Laws

Federal and State

- Complicated and conflicting patchwork of laws
- Special rules for certain industries, activities and data types
- Breach notification laws (47 states as of April 2014)
- FTC Enforcement under FTC Act §5 (unfair/deceptive trade practices)
- Increased focus on mobile privacy security and text message practices



HIPAA & Social Media

- ✓ The Basic HIPAA Privacy Rule:

A Covered Entity (CE) or its Business Associate (BA) may not *use or disclose*
Protected Health Information (PHI)
 unless the use or disclosure is specifically permitted by HIPAA.

- ✓ The HIPAA Security Rule requires all Electronic PHI be protected.

Any information, whether oral or recorded in any form, related to the mental or physical health condition of an individual, which identifies **or could be used to identify** an individual, and which is created, used, maintained or transmitted by or on behalf of a CE.



Examples of PHI

- Names
- Addresses (including city, county and full zip codes)
- Dates Directly Related to Patient (including DOB, DOS and all ages over 89)
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Numbers
- Account Numbers
- Certificate/License Numbers
- VINs, License Plate Numbers
- Device Identifiers and Serial Numbers
- URLs
- IP Addresses
- Biometric Identifiers (finger and voice prints)
- Full Face Photographic Images

What Disclosures are Permitted (Without Patient Authorization)?

- To the Individual
- For Treatment, Payment and Health Care Operations (TPO)
- *Incidental* Uses and Disclosures
- Uses and Disclosures with Opportunity to Agree or Object
- Public Interest and Benefit Activities
- Limited Data Set (under certain circumstances)

Note: Can also disclose to Business Associates if a proper Business Associate Agreement is in place.

Nursing Home surveys and deficiencies

- Privacy and confidentiality (483.10 [Resident Rights])
- Abuse, neglect, exploitation (483.13)
- Investigation and reporting of abuse allegations (483.13)
- Dignity, self-determination (483.15 [Quality of Life])

Criminal Charges

Many State criminal laws may be used to prosecute employees who post photos/videos of residents on social media:

- Elder abuse/failure to report
- Disorderly conduct
- Voyeurism
- Battery (when video show hitting)
- Invasion of privacy
- Taking a nude photo without consent
- Using a computer to commit a crime



17

ProPublica Study

- Episodes of nursing home or assisted living staff sharing photos or videos of residents on social media (January 2012-February 2016)
- 37 examples



18

ProPublica Study

- Photos/videos of residents using bathroom, showering, getting incontinent care
- Employees hitting, taunting, abusing residents; posing residents in crude situations; coaching residents to say "gangsta rap" song lyrics
- Employees doing/posting something positive [holding hands with residents; "This is my friend"] but posting without permission
- Photos/videos of staff (no residents) but charts/records visible



19

ProPublica Study

- 37 examples become **public knowledge**
 - 25 examples resulted in government inspections
 - 14 examples resulted in criminal charges
 - 18 examples resulted in news stories about the facility
- (total more than 37 because some examples result in 2 or 3 outcomes)



20

Freedom from Abuse, Neglect, and Exploitation (42 CFR § 483.12)

▪ *Reporting:*

- “We agree that abuse enabled through the use of technology would include the use of social media, as well as the use of cameras or the Internet. Following the publication of the final rule, we will release updated interpretive guidance that will aid facilities in implementing these regulations and provide further clarification for this regulation.”

21

Freedom from Abuse, Neglect, and Exploitation (42 CFR § 483.12)

▪ *Reporting:*

- “We believe that the use of technology to harm a resident is covered by the definition of ‘abuse’ which speaks specifically to abusive situations facilitated through technology.”
- “It includes verbal abuse, sexual abuse, physical abuse, and mental abuse including abuse facilitated or enabled through the use of technology.”

22

Freedom from Abuse, Neglect, and Exploitation (42 CFR § 483.12)

▪ *Reporting of Crime:*

- “We note that all allegations of abuse, with or without injury, fall into the immediate reporting category, as we believe it is imprudent to allow delay reporting of any abuse. Furthermore, we note that the 2-hour and 24-hour time frames represent maximums, and we would expect that most reports would occur more quickly.”

23

Nursing Home Surveys and Deficiencies

- CMS issued new memo to survey agencies, S&C:16-33-NH on August 5, 2016
- Definition of **mental abuse** includes staff taking or using photos or recordings in any manner that would demean or humiliate a resident—and—keeping or distributing photos/recording on social media
- Surveyors will investigate for abuse if a photo/recording demeans or humiliates a resident, **regardless of consent or cognitive ability**

24

Nursing Home Surveys and Deficiencies

- Nursing homes must **review/revise written abuse prevention policies and procedures** to address prohibition on taking or using photos/recordings in any manner that would demean or humiliate a resident
- Nursing homes must **train staff** on prohibition of taking, using, keeping, or distributing any photos/recordings demeaning or humiliating to a resident

25

Settlement/ Enforcement Actions

- **CardioNet – April 2017**
- First settlement involving wireless health services provider - \$2.5 million; unencrypted laptop stolen from workforce member's car
- OCR noted that CardioNet's risk analysis and risk management processes were insufficient and its HIPAA Security Rule policies and procedures were still in draft form

26

Settlement/ Enforcement Actions

- **Metro Community Provider Network – April 2017**
- Agreed to settle with OCR for \$400,000; hacker accessed employees' email accounts through a phishing email
- OCR noted that the settlement amount takes into consideration MCPN's status as a federally qualified health center

27

Settlements/ Enforcement Actions

- **Presence Health – January 2017**
- First settlement involving untimely breach notification – \$475,000; involved missing paper-based operating room schedules that contained the ePHI of 836 individuals
- Presence failed to timely notify individuals, the media and OCR
- OCR noted that Presence also failed to timely notify individuals with respect to several under 500 breach reports submitted during 2015 and 2016

28

Defining a HIPAA Breach

“Breach” means the acquisition, access, use or disclosure of unsecured PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of such information.

29

Breach Notification Rule

Breach Safe Harbor: Encryption and destruction are the only 2 methods to “secure” PHI – which is exempt from notification requirements

▪ **Three exceptions:**

- (1) Unintentional acquisition, access or use of PHI by a workforce member in the scope of duties – no further access or disclosure
- (2) Inadvertent disclosure from one authorized person to another within a CE/BA – no further access or disclosure
- (3) Disclosure of PHI where CE/BA has good faith belief that the recipient cannot retain the information

30

Breach Notification Rule

Risk Assessment –

Factors that must be considered:

- Nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

31

Breach Notification Rule

- CE/BA can decide to notify WITHOUT conducting a risk assessment
- Notice to affected individuals without unreasonable delay and no later than 60 calendar days from the date the breach was discovered (date knew or by exercising reasonable diligence should have known)
- Notice to HHS (less than 500 records) has to occur within 60 days of the end of the year in which breach was “discovered,” not in which it “occurred”
- Notice to HHS and the media may be required when 500 or more individuals are affected

Note: Must also consider state breach notification laws

32

Information OCR Requests

- Name and contact information of individual designated to work with OCR
- Position statement
- Business Associate Agreement (if applicable)
- Policies and procedures
- Evidence of workforce training
 - Training materials
 - Workforce attendance
- Evidence of sanctions (if applicable)



33

33

Information OCR Requests

- Security Rule cases
 - Risk analysis (be prepared to go 6 years back)
 - Risk management plan
 - Evidence of implemented security measures
 - Security incident report
- Breach cases
 - Notices to individuals and media
 - Evidence of corrective action



34

34

Preparing the Response

- Do not leave room for OCR to follow up with questions → anticipate questions in advance
- Be transparent → if you revised a policy after a breach, produce it
- Review OCR corrective action plans → ask yourself, what could they ask me to do in a CAP and voluntarily do it
- Bridge the gap with IT – if you don't understand your documentation, an investigator won't either



35

35

Key Tips for Avoiding Costly Settlements

- Encrypt! → safe harbor = no breach reporting obligation
- Take each incident (small or large) seriously → document corrective action
- Conduct a Risk Analysis and mitigate identified risks on an ongoing basis
- Proactively prepare
 - Cyber attacks
 - Breach Response



36

36

Key Tips Continued

- Review and organize your policies and procedures, BAAs, and other key documentation
- Train and re-train your employees
 - Valuable even if your organization is never selected for an audit. Will help decrease risk of breaches and complaints
 - Learn from mistakes of other organizations and use as teaching opportunities

37

BIPA
BIOMETRIC INFORMATION PRIVACY ACT
740 ILCS 14/1 *et seq.*



38

The Highpoints:

- Definitions:
 - **Biometric Information:** any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual!
 - **Biometric Identifier:** retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry
- Exceptions:
 - Demographic or physical descriptions
 - GINA or HIPAA
 - Image/Film Used to Diagnose, Treat, Test or Screen

39

The Highpoints

- Requirements:
 - Written Retention & Destruction Policy
 - Notice & Consent
 - Prohibition on Sale and Re-disclosure
 - Adequate Safeguards
- Penalties:
 - **Negligent** - \$1,000 or actual damages (whichever is greater)
 - **Intentional/Reckless** - \$5,000 or actual damages (whichever is greater)
 - **PLUS:** reasonable attorneys' fees and costs (including expert witness fees and other litigation expenses) and other relief (including an injunction as the court may deem appropriate).
- Plaintiff's Bar in Illinois

40

What Constitutes a Biometric?

- Retina or Iris Scan
- Fingerprint or Handprint
- Voiceprint
- Hand or Face Geometry
- Unique biological patterns or characteristics used to identify an individual
- Dental Biometrics?



Timekeeping Danger Zone



Developing Case Law

- Six Flags
- Google
- White Castle
- Black Horse Carriers



Social Media



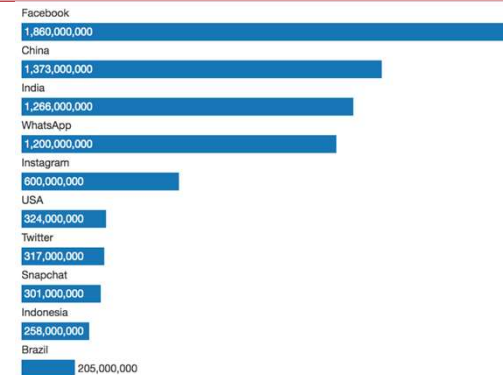
Social Media Use and the NLRB

- "Whether or not you are represented by a union, federal law gives you the right to join together with coworkers to improve your lives at work - including joining together in cyberspace, such as on Facebook."
- "Using social media can be a form of protected concerted activity. You have the right to address work-related issues and share information about pay, benefits, and working conditions with coworkers on Facebook, YouTube, and other social media."



45

Pretty Much Everyone is On Social Media



46

Nothing Stays in Vegas

- Social media enters the workplace, regardless of whether you intend it to.
- Comments and conduct that would be inappropriate at work, do not suddenly become appropriate because they are made via social media.



47

Danger of Electronic Communication: No Context

- Humor often does not translate through written communication.
- Absent context, otherwise innocuous texts or e-mails can be misconstrued or twisted to something offensive.



48

Facebook Whoops-a-daisy



POLSINELLI. What a law firm should be.

49

Protected Activity?

- A long time employee at a vegetable packing plant complained to managers and co-workers on several occasions about what he claimed were unsafe working conditions.
- Employee ultimately contacts the county health department to complain about rusted ammonia pipes.
- Two days later, the employee allegedly leaves his work post, yells at his supervisor, and is subsequently terminated.

POLSINELLI. What a law firm should be.

50

Boss Giving You A Hard Time? There's An App For That!



POLSINELLI. What a law firm should be.

51

NLRB Applies Expansive Social Media Rules

- Any action that employees could “reasonably construe” as restricting Section 7 Rights is prohibited.
- Of 20 social media policies reviewed by GC, only 4 found to be lawful.
- Employers must focus on why the content was impermissible.

POLSINELLI. What a law firm should be.

52

52

Back To the Future – Great Scott!

• Triple Play Sports Bar & Grille

- NLRB ruled that an employee "liking" a Facebook status is engaging in protected concerted activity

• Pier Sixty, LLC

- Employee states on Facebook that manager is a "Nasty Mother F---er" and "F--- his mother and his entire f---ing family"
- Board found it to be concerted protected activity



A Tale of Two Tweets

- "I was happy to see that Knauz went 'All Out' for the most important launch of a new BMW in years,"

- "This is your car. This is your car on drugs."



Critical Factors

- Does it affect terms and conditions of employment?
- Do co-workers comment? (if no comments, then no concerted activity in some cases)
- Can lose protection if comments are, among other things, scornful or disloyal
- Individual gripe—or commenting on terms and conditions?

Readiness Checklist


- ☐ Succinct social media policy?
- ☐ Prohibit cell phones on the floor?
- ☐ Completed a risk analysis?
- ☐ Current BAAs in place for all Business Associates?
- ☐ Cell phones and laptops are encrypted?

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.



57




POLSINELLI.
What a law firm should be.™

Where great work and great people come together.

Am Law 100 firm with
1,000 attorneys nationwide
23 offices from LA to NY
170+ services/industries
polsinelli.com

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements. Copyright © 2022 Polsinelli PC. All rights reserved. L.L.P. or California, Polsinelli PC, New York, N.Y.

58



Polsinelli PC provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

© 2022 Polsinelli® is a registered trademark of Polsinelli PC, Polsinelli LLP in California, Polsinelli PC (Inc.) in Florida.

polsinelli.com

59