BlueCross BlueShield | 2019 NATIONAL SUMMIT

Prickly Privacy Problems for Perplexed Plan Personnel

Tom Bixby
Thomas D. Bixby Law Office LLC
tbixby@tbixbylaw.com
(608) 661-4310

BOLD VISION. BROAD IMPACT.

Perplexed Plan Personnel's Personal Pet Peeve Privacy Problems?

BlueCross BlueShield | 2019 NATIONAL SUMMIT

How Helpful is Hashing?
Advertising on Social Media

BlueCross BlueShield | 2019 NATIONAL SUMMIT

Marketing: Advertising on Social Media!

Create a custom audience—target our Members

Target Social Media users who are not our Members

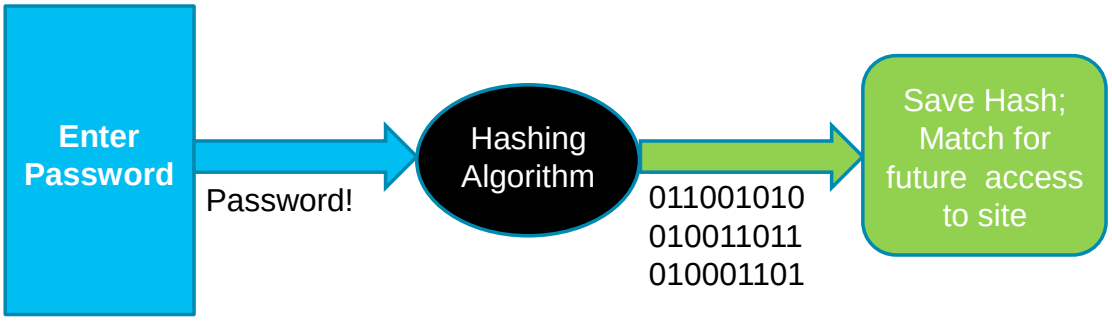
Provide Membership list to Social Media

- Not a business associate
- But they will HASH the data
- So "***no disclosure*** of protected health information"

BlueCross BlueShield | 2019 NATIONAL SUMMIT

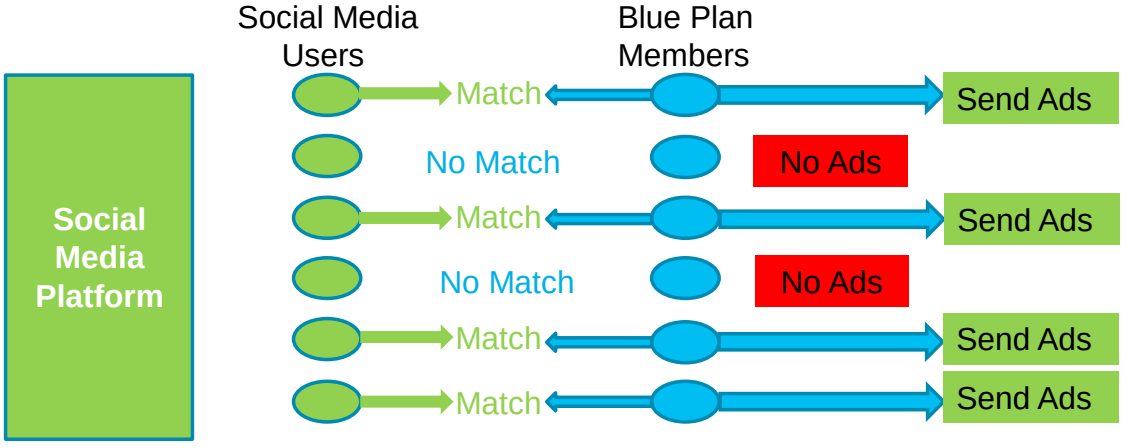
What is “HASHING”?

- Process used for passwords
  - Algorithm converts password to binary (base 2) number
  - Process allows storage of password without revealing password



How does Social Media use Hashing?

- Matching Social Media Users to Blue Plan Members



How does Hashing help?

Hashed information is ***not*** de-identified

- Hashed information contains identifiable data elements

Hashed information is not encrypted

- Encryption is different process
- Social media has the “key” for “decryption”

Social Media is not a business associate

- No restrictions on use or re-disclosure of Hashed information

Disclosing Data to Demanding Dealers

Big Data and the Deficit Reduction Act

BlueCross BlueShield | 2019 NATIONAL SUMMIT

Deficit Reduction Act Third-Party Liability

Vendor requests entire eligibility file on behalf of--

- Medicaid programs (in multiple States)
- Medicaid Managed Care Organizations (in multiple States)

Disclosure is "mandated" by Federal law

- Deficit Reduction Act of 2005

Data Use Agreement

- Data elements
- Data formats
- Frequency of updates

Application of HIPAA to TPL Data Requests

Required by Law

Disclosure must:

- Comply with applicable law;
- Be limited to relevant requirements of law

No Minimum Necessary

- But “relevant requirement” limitation is similar

Payment Activity

Payment Activities Include:

- Determinations of eligibility or coverage; and
- Coordination of benefits

Minimum necessary applies

Does Deficit Reduction Act Mandate Disclosure?

Social Security Act § 1902*

(a) A State plan for medical assistance must—

. . . .

(25) Provide—

. . . .

(I) that the State shall provide assurances satisfactory to the Secretary that ***the State has in effect laws*** requiring health insurers . . . ***as a condition of doing business in the State***, to:

(i) provide, with respect ***to individuals who are eligible*** [for Medicaid], information to determine during what period the individual . . . may be covered by a health insurer.

** 42 U.S.C. § 1396a(a)(25)(I) (emphasis added).*

CMS Guidance on Medicaid Third-Party Liability

State Law controls

"states, as a condition of receiving federal [Medicaid funding, must] have laws in effect that require health insurers . . . to provide the state with . . . information [about] individuals who are eligible for . . . Medicaid."

The Deficit Reduction Act does not require insurers to do anything.

What data is required?

"State laws determine what information is required of the health plans."

"State law cannot reach beyond the entities that are 'doing business' in their states."

The Deficit Reduction Act does not dictate what data must be provided.

What do State Laws require?

Florida

- "provide such records and information as are necessary" for Third-Party Liability determinations
- "unless such requirement results in an unreasonable burden."

Requirements of Data Use Agreement likely to result in unreasonable burden.

Wisconsin

"provide information . . . necessary [to determine] whether a recipient is being or has been provided coverage"; and

If a recipient is (or was) covered, "the nature and period of time of any coverage."

Information about a recipient not consistent with entire eligibility file.

Questions to ask about Third-Party Liability

For what States is data being requested?

- Are we “doing business” in that State?

What is required in States in which we do business?

- Information concerning “a recipient”? Or broader?

Are requested data elements reasonable under State law?

Alternative approach: Medicaid payment activities

- Eligibility inquiries (270/271 transactions?)
- Strict Data Use Agreement
- Medicaid disclosure of recipients for data match

Mechanics of Marketing Messages

What is (HIPAA) Marketing?

Making a communication about a product or service . . .

That encourages the recipient to purchase or use . . .

The product or service.

If use or disclose PHI in the process

Exceptions apply!

What does (HIPAA) Marketing include?

- Mailing to convert commercial members to Medicare
- Sending members Provider directories
- Case management/care coordination interactions
- Mailing for Value-Added Items & Services
- E-mail promoting life insurance product

"Marketing" is *prohibited* without member authorization

Marketing Exceptions:

No Remuneration

As long as there is ***no "financial remuneration"*** in exchange for making the communication,

THEN . . . .

"Financial remuneration" is direct or indirect payment from (or on behalf of) the third party whose product or service is being described in the communication.

Specific Exceptions

Communications permitted for:

- Health-related products or services provided by covered entity or included in benefit plan
- Participants in provider network
- Replacements/enhancements to health plan
- Value-Added Items & Services (with limitations)
- Case-management, care coordination

Marketing Checklist

For *any* communication sent to individuals, ask:

Are we using PHI?

- If not, no "marketing" issue

Does communication encourage recipient to use a product or service?

- If not, no "marketing" issue

Do we receive "remuneration" for sending communication?

- If yes, is the remuneration from a prohibited party?
- If yes, we have a "marketing" issue! Need authorization*

If the product or service is among the exceptions:

- Then no "marketing" issue;
- If not, we need individual authorization

Correctly Contracting with Clearinghouses
(and other third parties)

BlueCross BlueShield | 2019 NATIONAL SUMMIT

When is a Business Associate Agreement Necessary?

Common belief:

- No harm in requiring business associate agreement
- "I can't be blamed" if anything goes wrong

Business Associate Agreement

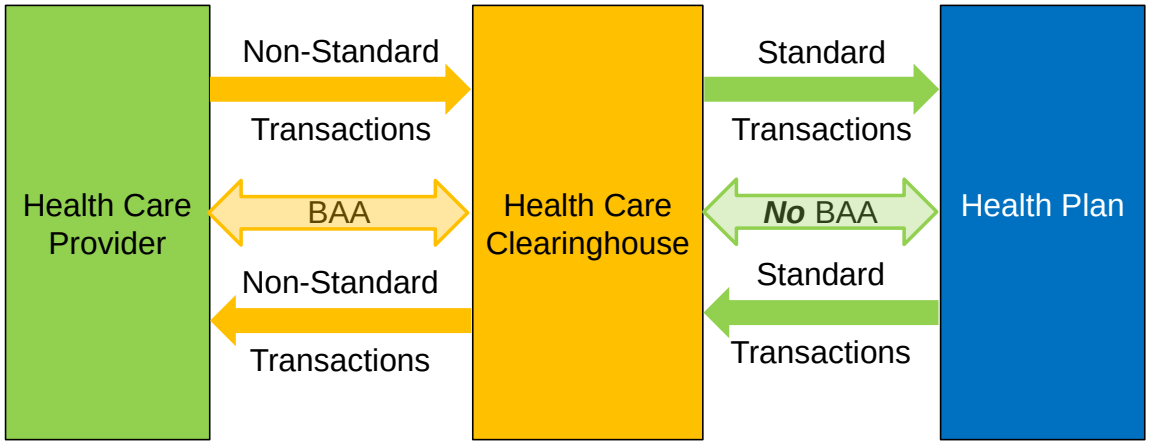
- *Does* impose safeguards on members' information
- *But* creates unnecessary risks when BAA is not required

When is a third party a business associate?

- **Two elements to be business associate:**
  - Perform on behalf of covered entity function or activity
  - Involves use, disclosure, maintenance, or transmission of PHI
- **Performs on behalf of Covered Entity**
  - Covered Entity's Payment activities
  - Covered Entity's Health Care Operations
  - [*Health Care Provider's Treatment activities*]

Clearinghouse Function

Convert non-standard Electronic Transactions into Standard Transactions



When is a BAA *not* necessary?

Disclosures to Covered Entity w/o BAA

- Health care clearinghouse (when sending standard transactions)
- Participating provider (when plan is BA)

When a disclosure is for *recipient's* TPO

Disclosures to other third parties w/o BAA

- Pharmaceutical Manufacturer
- Stop Loss Carrier
- Health oversight agency (*e.g.*, FBI)
- Bank (*i.e.*, check made out to member)

When recipient not performing on CE's behalf

Perplexed Plan Personnel's Personal Pet Peeve Privacy Problems?

Tom Bixby
tbixby@tbixbylaw.com
(608) 661-4310

Thank You

Tom Bixby
Thomas D. Bixby Law Office LLC
tbixby@tbixbylaw.com
(608) 661-4310

BlueCross BlueShield | 2019 NATIONAL SUMMIT