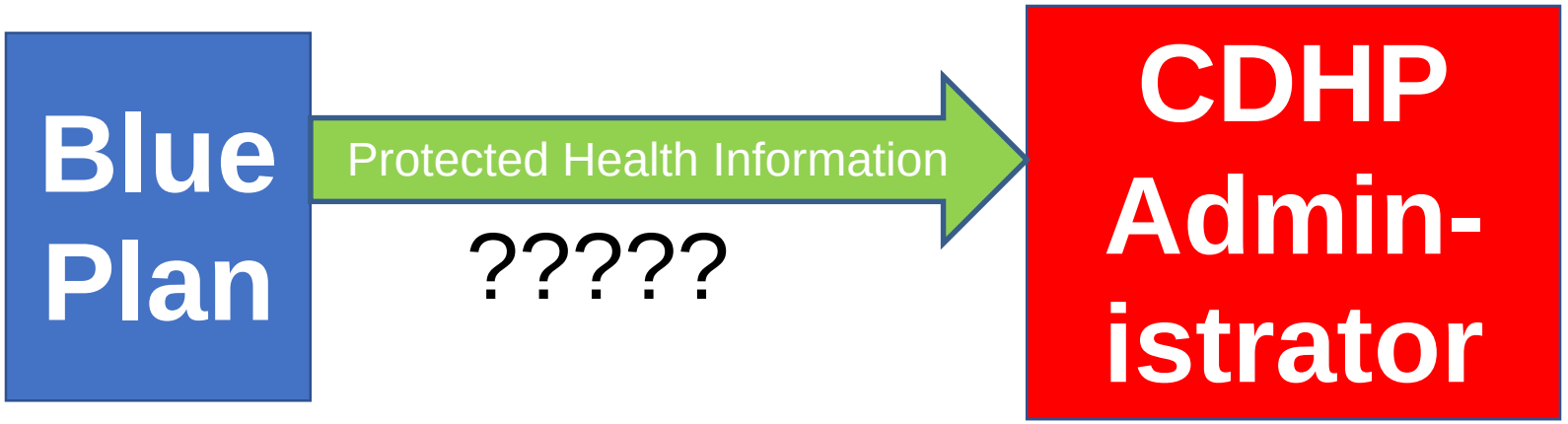
Disclosing PHI to a CDHP Administrator: How HIPAA Applies to FSAs, HRAs, and HSAs

Blue Cross Blue Shield Association
Legal Department Cooperative
Teleconference
November 2, 2017

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

When can I disclose PHI to a third party for the administration of FSAs, HRAs, & HSAs?



Topics

- Relevant HIPAA Rules
- FSAs, HRAs, and HSAs: What are they?
- Application of HIPAA to FSAs, HRAs
- Application of HIPAA to HSAs
- “But we can’t do that . . .”
- Questions

Relevant HIPAA Rules

Who is subject to Privacy Rule?

Covered entities/health plans

- Health insurance issuers
- HMOs
- [*Not Employers*]
- Employer sponsored group health plans

Business associates

- Perform function or activity ***on behalf of*** health plan
- Create or receive protected health information

Who is subject to Privacy Rule?

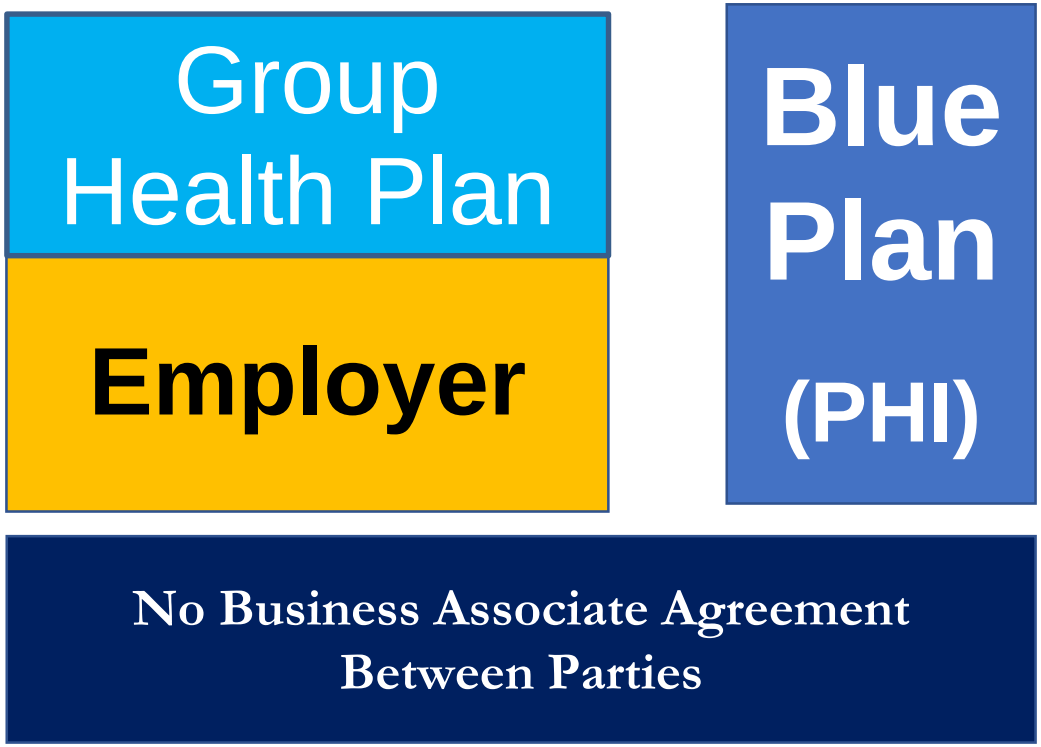
Fully-Insured group health plans

- (Virtually) No HIPAA compliance obligations
- Provided that, receive no PHI other than:
  - Summary health information
  - Enrollment/eligibility information

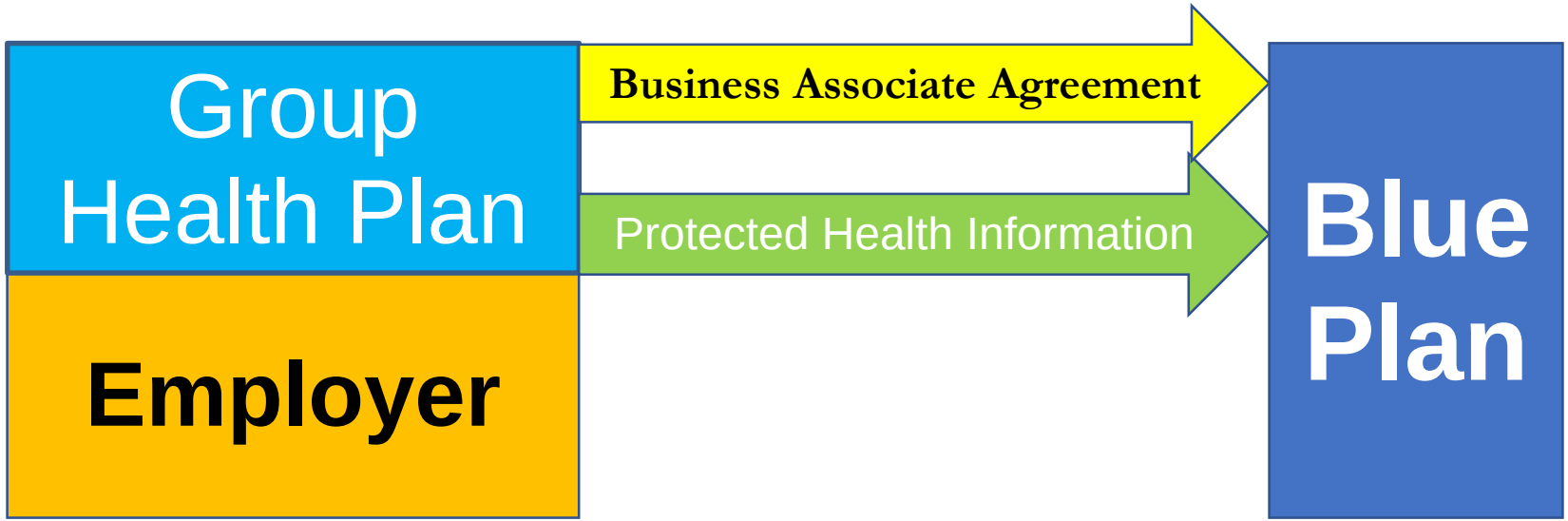
Other group health plans (*e.g.*, self-funded)

- Full compliance with HIPAA Rules

Fully-Insured Group (no PHI)



Self-Funded Group



Privacy Rule Starting Point:

No use or disclosure, unless

- Exception applies; or
- Member provides HIPAA-compliant authorization

Minimum necessary limitation

- Applies to most uses and disclosures
- May rely covered entity's request (if reasonable)
- May rely business associate's request (if reasonable)

Privacy Rule

Exception: payment activities

- May disclose PHI for recipient's "payment activities"
- May disclose to health plan's business associate

"Payment"

- Activities to determine or fulfill health plan's responsibility for coverage and provision of benefits

Privacy Rule

Disclosure by Authorization

- Specific information and disclaimers required
- Expiration date or event—State law impact?

Each individual must authorize

- Subscriber authorization vs. adult dependents
- Signature required (opt-in, not opt out)

Privacy Rule

Prior to any disclosure, must verify:

- Identity of recipient
- Authority of recipient to receive PHI

Disclose only minimum necessary

FSAs, HRAs, and HSAs
What Are They?

Consumer Directed Health Plans

Individual Accounts for Health Spending

- Controlled by member
- Pre-tax contributions (member, employer, or both)
- Spending only for Qualified Medical Expenses

Three types

- Flexible Spending Arrangement (FSA)
- Health Reimbursement Arrangement (HRA)
- Health Savings Account (HSA)

Consumer Directed Health Plans

Qualified Medical Expenses

- Deductibles
- Copayments/coinsurance

Popular features

- Automatic reimbursement
- Debit cards

Consumer Directed Health Plans

CDHP Administrators

- Contract with Employers (typically)
- Compete on ease of use (auto-pay, debit cards)

Data from Blue Plan is key

- Claim information needed for auto-pay/debit card
- Send us your Protected Health Information!

FSAs, HRAs, and HSAs

One of these things is not like the others,

One of these things just doesn't belong,

Can you tell which thing is not like the others?

By the time I finish my song?

Definitions

ERISA Employee Welfare Benefit Plan

- Established & maintained by Employer
- Plan, fund, or program—defined benefits & limitations
- Provide employees medical/health benefits

HIPAA group health plan

- ERISA employee welfare benefit plan
- Administered by third party

FSA/HRA

FSA/HRA is ERISA Benefit plan

- Established/maintained by employer
- Plan, fund, or program—defined benefits & limitations
- Provides employees medical/health benefits

FSA/HRA is HIPAA group health plan

- ERISA employee welfare benefit plan
- Administered by third party

FSAs and HRAs

HIPAA health plans and covered entities

- Comply with same HIPAA requirements as Blue Plan
- May disclose PHI for FSA/HRA payment activities

CDHP Administrator Role

CDHP Administrator is not covered entity

- ***Not*** a health plan
- ***Not*** a provider or health care clearinghouse

CDHP Administrator *is* business associate

- Uses/discloses protected health information
- Perform a function or activity
- On behalf of FSA/HRA—group health plan, But, ***not*** the business associate of Blue Plan

HSAs: Not like the others!

Health Savings Accounts

- Contribute to only when enrolled in HDHP
- Use funds at any time
- May invest funds
- Similar to 401(k)/IRA

Custodial Account Agreement

- Between “beneficiary” and account administrator

HSAs: Not like the others!

ERISA Employee Welfare Benefit Plan

- ***Not*** established & maintained by Employer
- ***Not*** plan, fund, or program

HIPAA group health plan

- ***Not*** a HIPAA group health plan (or covered entity)

HSA Administrator

- ***Not*** a health plan or covered entity
- ***Not*** a business associate

Application of HIPAA to FSAs and HRAs

HIPAA and FSAs/HRAs

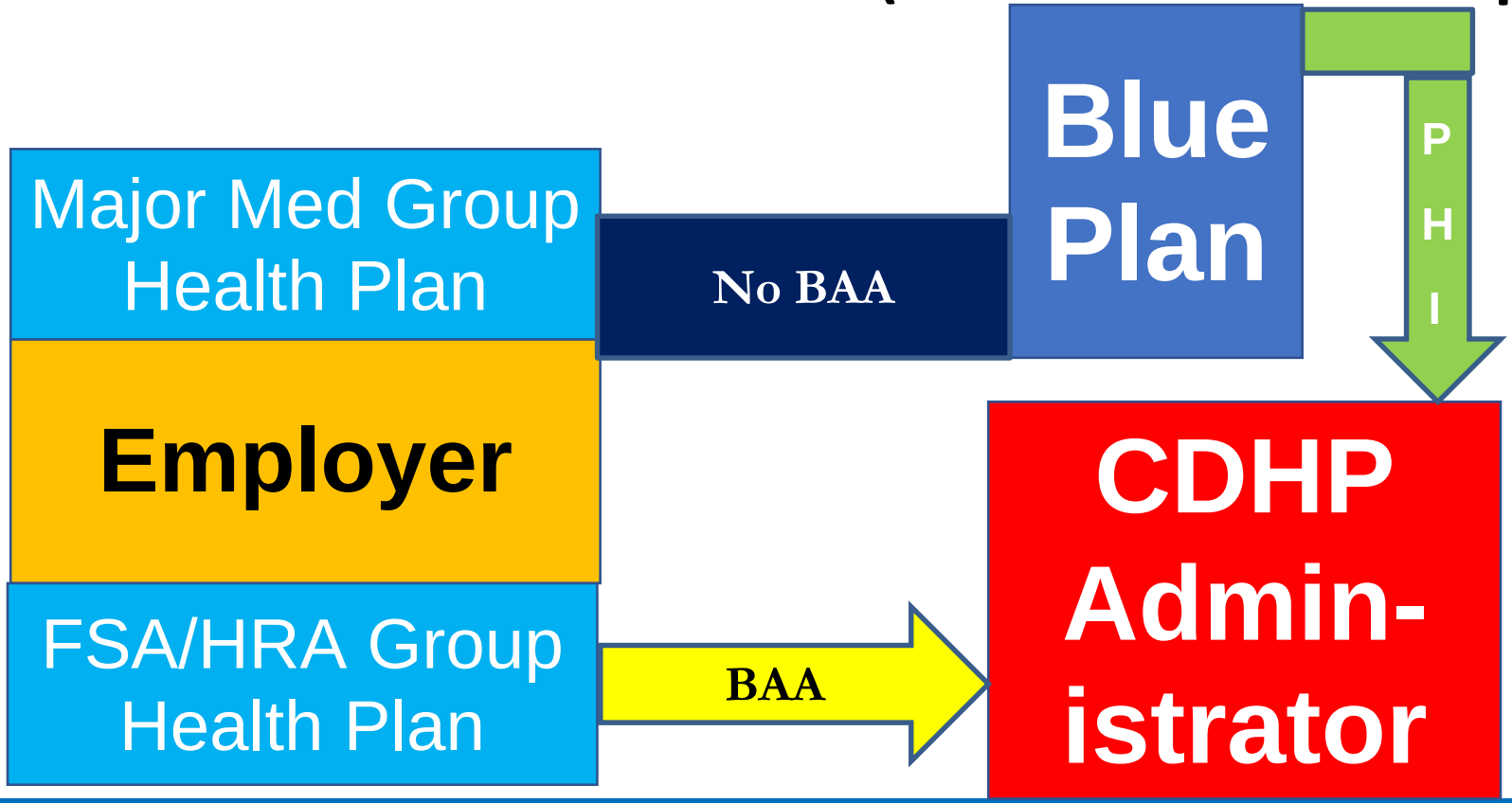
FSA/HRA is Group Health Plan

- Disclosure permitted for ***payment*** activities
- Processing members' claims is payment activity

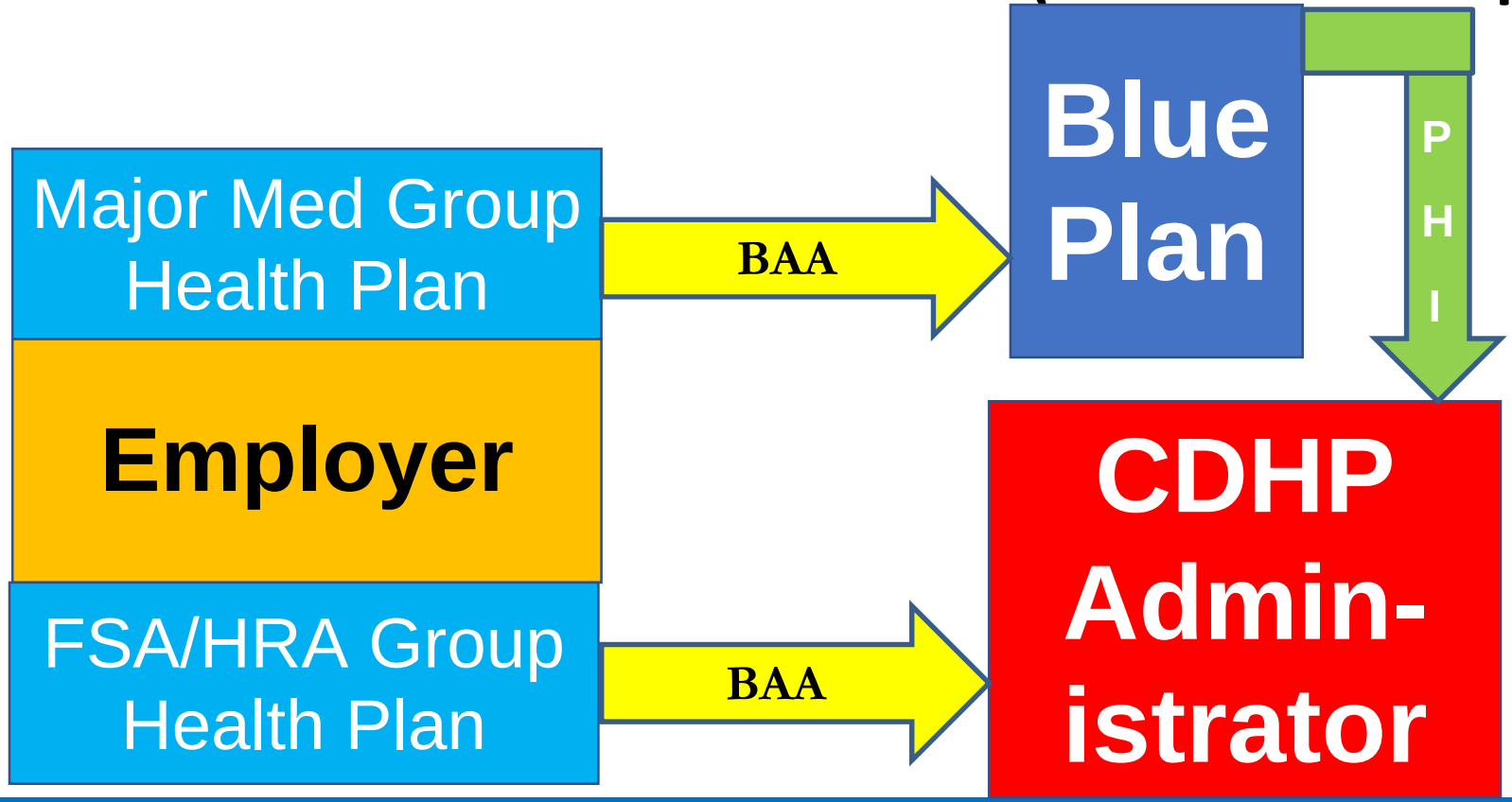
CDHP Administrator as business associate

- BAA with FSA/HRA—group health plan is required
- Blue Plan may disclose for "payment" activities

FSAs & HRAs (Insured Groups)



FSAs & HRAs (ASO Groups)



HIPAA and FSAs/HRAs

Minimum necessary limitation

- How much information is necessary?
- Whose information is necessary?
  - Dependents?
  - Employees/dependents not enrolled in FSA/HRA?

Rely on request from Administrator

- Provided that request is reasonable under the circumstances

HIPAA and FSAs/HRAs

Verification of recipient identity/authority

- Direction of employer-sponsored group health plan
- Business associate agreement with administrator
- Minimum necessary

Three-way agreement

- Blue Plan
- Employer
- CDHP Administrator

Application of HIPAA to HSAs

HIPAA and HSAs

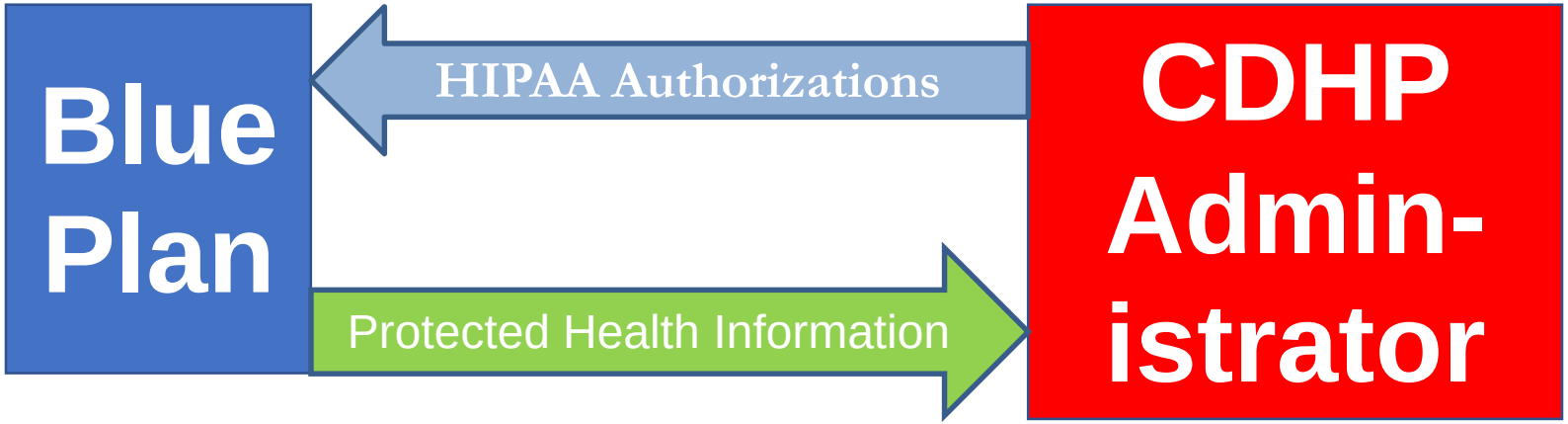
HSA is *not* Group Health Plan

- Disclosure not permitted (not "***payment***")
- No other applicable exception
- ***Authorization*** required

Whose authorization is necessary?

- Employee/subscriber
- Spouse/dependents
- Anyone whose PHI is disclosed

HSAs



No Business Associate Agreement Between Parties

HIPAA HSAs

Verification of recipient identity/authority

- Authorization from each affected member?
- HIPAA-compliant authorization?
- (Liability for failure to collect authorization?)

Three-way agreement

- Blue Plan
- Employer
- CDHP Administrator

But we can’t do that . . .

But we can't do that . . .

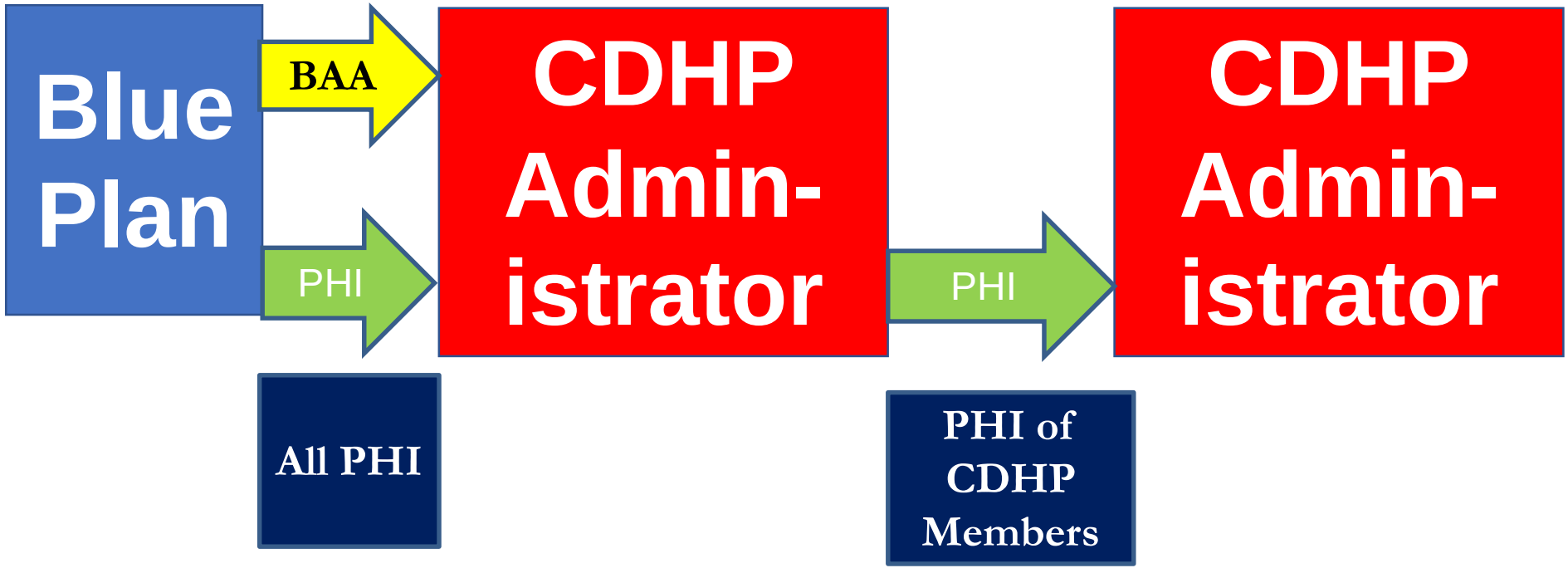
System not capable of:

- Providing PHI only for enrollees of FSA/HRA
- Providing PHI only for members signing authorizations (HSAs)

BAA with CDHP Administrator

- Administrator to sort PHI on Blue Plan's behalf
- "Re-disclose" PHI to Administrator
- No "Re-disclosure" of other PHI

“But we can’t do that . . .”



Questions

Disclosing PHI to a CDHP Administrator: How HIPAA Applies to FSAs, HRAs, and HSAs

Blue Cross Blue Shield Association
Legal Department Cooperative
Teleconference
November 2, 2017

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