HIPAA Update:
What's New with the Final Rule?

Sponsored by:

Washington State

Health Information Management Association

EvergreenHealth

Kirkland, Washington

April 12, 2013

CHRISTIANSEN IT LAW
WWW.CHRISTIANSENLAW.NET
Information Technology Law | Privacy / Security / Compliance | Contracting, Risk Management & Due Diligence

Presenter CV

John R. Christiansen, J.D. **- Christiansen IT Law**

- Special Assistant Attorney General to Washington State Health Care Authority, health care information issues related to HIPAA, HITECH, and related issues
- Privacy and Security Expert, ***ONC/OCR Comprehensive Campaign for Communication and Education About the HITECH Act*** (2010 – pres.); Consultant, ***ONC State Health Policy Consortium*** (2010 – pres.); Technical Advisor, ***ONC Health Information Security and Privacy Collaboration*** (2005 – 2009)
- Chair, ***ABA HITECH Megarule/Business Associates Task Force*** (2009 – pres.); ***Committees on Healthcare Privacy, Security and Information Technology*** (2004 – 06); on ***Healthcare Informatics*** (2000 – 04); and ***PKI Assessment Guidelines Health Information Protection and Security Task Group*** (2000 – 2003)
- Executive Committee/Secretary, **Washington State Bar Association Health Law Section** (2012 – pres.)
- Adjunct Faculty, ***University of Washington Information School*** (2008 – pres.); ***Oregon Health and Sciences University Division of Medical Informatics and Outcomes Research*** (2000 – 2003)
- Publications include ***State and Federal Consent Laws Affecting Health Information Exchange*** (Nat'l Governors Association 2011); ***Policy Solutions for Advancing Interstate Health Information Exchange*** (Nat'l Governors Association 2009); ***An Integrated Standard of Care for Healthcare Information Security*** (2005); ***Electronic Health Information: Security and Privacy Compliance under HIPAA*** (2000); etc.

Our Agenda

- HIPAA Baseline and HITECH Megarule Background
- HITECH changes to the Privacy Rule
- The New Business Associate Rules
- Changes to the Breach Notification Rule
- Trends in Enforcement and Penalties

HIPAA Baseline Review

- HIPAA – the Health Insurance Portability and Accountability Act of 1996
  - Privacy Rule – effective 2003
  - Security Rule – effective 2005
- HITECH – the Health Information Technology for Economic and Clinical Health Act; part of 2009 stimulus bill
  - Supplements and amends HIPAA

HIPAA Baseline Review

- HIPAA Basics
  - What is protected?
    - Protected Health Information (PHI) – essentially any patient information, in any medium (written, oral, electronic), maintained for any purpose
    - Medical and health records; administrative, operating, business, research records, etc., etc., etc.

HIPAA Baseline Review

- HIPAA Basics
  - Who is regulated?
    - Covered Entities (CE) – Any health care provider which gets paid electronically, health plans, health care clearinghouses
      - Directly regulated under HIPAA – subject to regulatory obligations and penalties
    - Business Associates (BA) – Any person or organization which obtains or uses PHI to perform a service or function on behalf of a Covered Entity; technology services providers, professional services providers, consultants, etc., etc.
      - Not directly regulated under HIPAA – no regulatory obligations or penalties
      - Indirect regulation by requirement that CEs must have Business Associate Contract (BAC) with BA

HIPAA Baseline Review

- HIPAA Basics
  - Who is regulated?
    - Covered Entities (CE) – Any health care provider which gets paid electronically, health plans, health care clearinghouses
      - Directly regulated under HIPAA – subject to regulatory obligations and penalties
    - Business Associates (BA) – Any person or organization which obtains or uses PHI to perform a service or function on behalf of a Covered Entity; technology services providers, professional services providers, consultants, etc., etc.
      - Not directly regulated under HIPAA – no regulatory obligations or penalties
      - Indirect regulation by requirement that CEs must have Business Associate Contract (BAC) with BA

HITECH Background

- The American Recovery and Reinvestment Act of 2009
  - H.R. 1, Pub.L. 111-5 (February 17, 2009)
  - “ARRA” or “the Stimulus Bill
  - 407 pages
- Title XIII of ARRA: Health Information Technology for Economic and Clinical Health Act
  - HITECH Act
  - 53 pages
- Subtitle D: Privacy
  - 21 pages

HITECH Background

- Principally intended as stimulus vehicle
  - Financial incentives for adoption of electronic health records (EHRs) and health information exchange (HIE)
  - Grant streams for development and implementation of EHRs, HIEs, demonstration projects, support tech curriculum development, etc.
  - Subtitle D drafted in haste and it shows
- Principal concepts
  - Move healthcare providers to EHRs and HIE
  - Extend regulation over key healthcare IT players (Business Associates)
  - Create new security breach notification requirements
  - Increase penalties and tighten enforcement
  - Tighten some PHI use and disclosure limitations
  - Tweak patient/consumer data access rights

HITECH Background

- Subtitle D structure:
  - Incorporates key HIPAA regulatory definitions by reference: CE, BA, PHI, Use, etc.
  - Adds new statutory requirements to existing HIPAA statutory and regulatory requirements
  - Mostly does not formally repeal or amend existing HIPAA requirements
    - Some implied amendments appear unavoidable
  - Requires some new regulations and some new regulatory guidance

HITECH Background

- Rules Required by HITECH
  - Security Breach Notification: Published 2009, updated by Megarule
  - Penalty Rule amendments: Published 2009, updated by Megarule
  - Business Associate amendments to Privacy, Security and Penalty Rules: Megarule
  - Fundraising, Marketing, Sales of PHI, Research, Genetic Information, Additional Restrictions: Megarule
  - Minimum Necessary: Pending
  - Accounting of Disclosures: Pending

HITECH Megarule Essentials

- Compliance Timing
  - Megarule officially published January 25 (unofficially January 18)
  - Official effective date is March 26
  - “Compliance Date” is September 23 (180 days from March 26)
    - For all regulations “that become effective after January 25, 2013, CEs and BAs must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications.”
    - No obligation to comply means no penalties for failure to comply

HITECH Megarule Essentials

- What the Megarule Added: For CEs
  - Miscellaneous minor changes to some disclosures
  - Marketing communications must disclose if CE receives third party remuneration
  - Fundraising communications must include opt-out
  - Some tweaks to Notice of Privacy Practices
  - Electronic records must be provided in electronic form if requested and “readily producible”
  - No disclosure to plans of information about treatment or services, upon request if paid for in full
  - No use of genetic information for insurance underwriting
  - A few other odds and ends
  - New BAC requirements – see below

HITECH Megarule Essentials

- What HITECH Added: For BAs
  - Many, many more BAs!
  - Old BA definition: BA is an entity which performs an activity or functions for or on behalf of or provides a service to a CE, which involves use or disclosure of PHI
    - Remember: Under old rules BAs are not regulated, BACs provide indirect regulation
  - New BA definition: Summarize as any party which obtains PHI to use or disclose to perform function or activity for or on behalf of, or provide services to or for the benefit of, a CE, directly or indirectly
    - BAs are now both directly regulated, and indirectly by BAC
    - Many complexities; see lengthy discussion below

Fundraising

- Definition and Scope of "Fundraising": Not Changed
  - "A communication to an individual that is made by a covered entity, an institutionally related foundation, or a business associate on behalf of the covered entity for the purpose of raising funds for the covered entity is a fundraising communication[.]"
  - "Permissible fundraising activities include appeals for money, sponsorship of events, etc. They do not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc.).''
  - Requires either individual authorization, or compliance with fundraising rules below

Fundraising

- Definition and Scope of Authorized PHI: Expanded
- "[A] covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following [PHI] for the purpose of raising funds for its own benefit, without an authorization . . .
    - Demographic information relating to an individual, **including name, address, other contact information, age, gender, and date of birth**; and
    - Dates of health care provided to an individual;
    - **Department of service information;**
    - **Treating physician;**
    - **Outcome information; and**
    - **Health insurance status**."
- Make sure Minimum Necessary policies conform to rule

Fundraising

- Conditions to Fundraising Communications: Tweaked
  - CE Notice of Privacy Practices must include a statement to the effect that:

    "The covered entity may contact the individual to raise funds for the covered entity **<u>and the individual has a right to opt out of receiving such communications."</u>**
  - "A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fund-raising communications."
  - Each fundraising communication must include a "a clear and conspicuous opportunity to elect not to receive any further fundraising communications."

Fundraising

- Opt-Out Requirements: Tweaked/Clarified
  - Opt-out may apply to all future communications, or campaign-specific communications – but "the communication should clearly inform individuals of their options and any consequences of electing to opt out of further fundraising communications."
  - Opt-out processes which do not create "an undue burden or more than a nominal cost."
  - Examples:
    - Toll-free or (free/cheap) local phone number
    - Email
    - Pre-printed/prepaid postcard
    - Requiring individual to write and send a letter ***not*** permitted
    - Multiple options may be permitted
  - Opt-back-in process is permitted

Fundraising

- Organizational Arrangements for Fundraising
  - Internal unit of CE
  - Institutionally related foundation
  - BA contracted to Covered Entity - not an institutionally related foundation

Fundraising

- Organizational Arrangements: Internal Unit of CE
  - Hybrid entity rules: Not changed
  - CE designates “health care components” by policy, internal arrangements
  - Health care components perform covered functions (e.g. health care)
  - Other components perform other, non-covered functions (e.g. fundraising)
  - Health care components may only disclose PHI to non-health care components in compliance with Privacy Rule (e.g. applicable to fundraising)
  - Non-health care components may only use PHI in compliance with Privacy Rule

Fundraising

- Organizational Arrangements: Institutionally Related Foundation
  - Not changed
  - Not a BA due to Internal Revenue Code prohibitions, so not subject to the new BA rules
  - “A foundation that qualifies as a nonprofit charitable foundation under section 501(c)(3) of the Internal Revenue Code and that has in its charter statement of charitable purposes an explicit linkage to the CE.”
  - “The term does not include an organization with a general charitable purpose, such as to support research about or to provide treatment for certain diseases, that may give money to a covered entity, because its charitable purpose is not specific to the covered entity.”
  - Use, disclosure of PHI by foundation is controlled by agreement with CE
  - Will state attorneys general enforce HIPAA/HITECH against foundations?

Fundraising

- Organizational Arrangements: BAs
  - See discussion below
  - Make sure BACs pass along appropriate Minimum Necessary policies, requirements for BA to comply with CE Fundraising requirements

Marketing

- CE must have an individual's authorization before the CE or a BA on behalf of the CE engage in "marketing" to the individual
  - "Marketing:" "Communication about a product or service that encourages recipients of the communication to purchase or use the product or service."
  - Limitations on "financial remuneration" to CE for marketing
    - "Financial remuneration:" "Direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual."

Marketing

- Exceptions from "Marketing:"
  - Any of the following, unless the CE "receives financial remuneration in exchange for making the communication:"
    - Treatment by a health care provider, including direction or recommendation of alternative treatments, therapies, health care providers, or settings of care
    - Description of benefit plan products, services, or payment terms, including e.g. PPO and other network providers, changes to benefits, value-added products and services, etc.
    - Case management and care coordination, whether defined as treatment or otherwise

Marketing

- Exceptions from “Marketing:”
  - Refill reminders or comparable communications about current prescriptions,” as long as “any financial remuneration received by the CE in exchange for making the communication is reasonably related to the CE’s cost of making the communication.”
  - CE no longer required to include notice of possible use of PHI to give appointment reminders, etc. in Notice of Privacy Practices

Sales of PHI

- CEs and BAs May Not “Sell” PHI without Authorization
  - “Sale:” “A disclosure of PHI by a CE or BA, where the CE or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.”
  - “Remuneration:” ***Not*** the same as marketing “financial remuneration.” Includes direct and indirect, financial or nonfinancial “benefits,” received from PHI recipient or any other party
  - Authorization must include statement that CE will receive remuneration

Sales of PHI

- Exceptions to “Sale of PHI”
  - Disclosure for purposes of public health activities
  - Disclosure for research purposes where the only remuneration is “a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes”
  - Disclosure for treatment and payment purposes
  - Disclosure for the “sale, transfer, merger, or consolidation of all or part of the CE and for related due diligence”
    - But not for a BA?

Sales of PHI

- Exceptions to “Sale of PHI”
  - Disclosure to or by a BA for activities on behalf of a CE, or on behalf of a BA in the case of a subcontractor, if remuneration is solely for the activities
  - Disclosure to the individual upon request
  - Disclosure “required by law”
  - Disclosure for any other purpose permitted under and in accordance with the Privacy Rule, “where the only remuneration . . . is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law”

Sales and Marketing Sample Problems

- PHR Vendor and Patient Ads
  - PHR provided by vendor to patients, as service to their physician practice
    - Vendor is BA under the new BA rules
  - Vendor provides service free because it is supported by advertising on patient pages
    - Is this marketing? Is it sale of PHI?

- The Ad-Supported EMR
  - EMR provided by vendor as service to physician practice
  - Vendor provides service free because it is supported by advertising on patient medical record screens
  - Advertising is targeted by words and phrases on screen
    - Is this sale of PHI?

Additional Restrictions on Disclosure of PHI

- Genetic information: May not be used by a health plan, other than a long-term care plan, for underwriting purposes
- Underwriting includes:
  - Coverage, benefits, cost-sharing determinations and rules
  - Premium determinations
  - Application of pre-existing condition exclusions
  - Any other activity related to insurance contract or policy creation, renewal or placement
- Underwriting does not include determinations of medical appropriateness

Additional Restrictions on Disclosure of PHI

- Genetic information includes:
  - An individual's genetic tests
  - Genetic tests of family members, including a fetus or embryo "legally held by an individual or family member utilizing an assisted reproductive technology"
  - Manifestation of a disease or disorder in family members
  - Any request for, receipt of genetic services, participation in clinical research including genetic services, by individual or family member
- Genetic information excludes information about sex or age .

Additional Restrictions on Disclosure of PHI

- Genetic services includes:
  - Genetic counseling
  - Genetic education
  - Genetic test: "An analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes"
    - "Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition"
      - "Manifestation or manifested:" "Individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved . . . a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information"

Additional Restrictions on Disclosure of PHI

- Services paid out-of-pocket
  - CE must agree to request not to disclose PHI to health plans if:
    - Disclosure is for payment or health care operations and is not required by law; and
    - “PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the CE in full”
  - Can you tag/segment such data in electronic records?

Easing of Restrictions on Research

- Prohibition on Combining “Conditioned” and “Unconditioned” Authorizations Removed
  - “Combined” authorizations: Authorization for two different purposes
  - Generally prohibited – general prohibition continues
  - Research exception: May combine research authorization (informed consent) + other authorization
  - May not combine “conditioned” and “unconditioned”
    - “Conditioned:” Authorization required for treatment, payment, enrollment, eligibility
    - “Unconditioned:” Authorization fully optional

Easing of Restrictions on Research

- Sample problem of compound authorization prohibition
  - Study participants to receive experimental treatment, contribute tissue specimens for reference
  - Experimental treatment requires informed consent: Treatment requires authorization for PHI use for research purposes
    - Conditioned authorization
  - Use of PHI related to tissue specimen does not
    - Unconditioned authorization
  - Old rule: Two authorization forms required
  - New rule: Both conditioned and unconditioned authorizations may be combined
    - Some reasonable explanation of distinction required: Check box, separate page, etc. as reasonably determined by IRB, CE, etc.

Easing of Restrictions on Research

- Prior Interpretation of Privacy Rule Prohibiting Authorization for Future Research Reversed
  - Not a regulation
  - Prior interpretation required authorization to apply only to specific study
  - New interpretation permits application to future research as described in authorization

Declassification of Decedent Information as PHI

- Old rule: PHI is PHI forever – Privacy Rule applies, decedents' personal representative must authorize use/disclosure if exception does not apply
- New rule: PHI is PHI until 50 years from date of decedent's death

Provision of Records

- CE must provide access to PHI “in the form or and format requested . . . if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or and format as agreed to by the CE and the individual”
  - If PHI maintained in electronic form in designated record set, must be provided in electronic form, likewise as requested “if readily producible and otherwise as agreed”
  - CE must transmit PHI to third party upon clear, written, signed direction by individual

The Old BA Regime

- Background: HIPAA Jurisdictional Limitations and the BA Workaround
- HIPAA Administrative Simplification intent: Require implementation of electronic health claims transactions
  - Privacy and Security Rules: Ancillary trust builders which grew beyond expectation
- Covered Entities (CE):
  - Organizations directly involved in health claims transactions
    - Any health care provider which gets paid electronically, health plans, health care clearinghouses
    - Directly regulated under HIPAA – subject to regulatory obligations and penalties

The Old BA Regime

- HIPAA Jurisdictional Limitations and the BA Workaround
  - CEs don’t/can’t perform all functions and activities involving use or disclosure of PHI by themselves
  - How to protect PHI when non-CEs must access or control it?

The Old BA Regime

- Old BA Definition
  - A “person” who is not a CE workforce member and:
    - “Performs or assists in the performance of” a function or activity involving the use or disclosure of PHI on behalf of a CE
      - Official examples: Claims processing or administration; data analysis, processing or administration; utilization review; billing; quality assurance; benefit management; practice management, repricing
      - Any other “function or activity “ regulated under HIPAA
        - My examples: PHI disclosure to other CEs, individuals, public health, research, marketing, etc.; security management and administration; etc.
    - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services on behalf of a CE, involving disclosure of PHI for purposes of the services to the BA by the CE or another BA

The Old BA Regime

- Business Associate Contracts (BACs) and the BA Workaround
  - CE may disclose PHI to/allow BA to create or receive PHI on CE's behalf upon "satisfactory assurance" BA will "appropriately safeguard" PHI
    - 45 CFR § 164.502
  - "Satisfactory assurance" is BAC including required provisions (or equivalent memorandum of understanding if governmental entities, plan document provisions if group health plan)
    - 45 CFR § 164.504(e)

- BA status is "definitional," does not depend on existence of BAC
  - If it does what a BA does, it's a BA
  - Knowledge or intent of CE or BA are irrelevant

The Old BA Regime

- Business Associate Contracts (BACs) and the BA Workaround
  - Governmental agencies acting as CEs and BAs must also implement BAC via memoranda of understanding or comparable documentation
  - Group health plans making PHI available to administration by sponsor must implement BAC equivalent in health plan documents

The Old BA Regime

HIPAA BAC Content	
REQUIRED: Define permitted uses and disclosures of PHI for purposes of underlying agreement	**REQUIRED:** BA must provide information needed for accounting of disclosures by CE
REQUIRED: No prohibited use or disclosure of PHI by BA	**REQUIRED:** BA must make internal books, records, etc. available to DHHS for determination of CE compliance
REQUIRED: BA must use “appropriate” safeguards to prevent use or disclosure of PHI other than as permitted by BAC or required by law	**REQUIRED:** BA must return or destroy all PHI upon termination of BAC, or may escrow if return or destruction not feasible
REQUIRED: BA must comply implement administrative, physical and technical safeguards to reasonable and appropriately protect confidentiality, integrity, availability of electronic PHI	**REQUIRED:** BAC must allow CE to terminate BAC for BA violation
REQUIRED: BA must report security incidents to CE	**OPTIONAL:** BA may use PHI, “if necessary,” for BA’s “proper management and administration”
REQUIRED: BA must ensure that any subcontractor or agent to which it provides PHI implements “reasonable and appropriate safeguards” to protect it	**OPTIONAL:** BA may use PHI, “if necessary,” to “carry out the legal responsibilities of the BA”
REQUIRED: BA must ensure that any subcontractor or agent to which it provides PHI “agrees to the same conditions and restrictions that apply to the BA” under the BAC	**OPTIONAL:** BA may disclose PHI “if required by law”
REQUIRED: BA must make any PHI in designated record set (DRS) available for individual access	**OPTIONAL:** BA may disclose PHI to for BA’s management, administration, legal responsibilities, upon “reasonable assurances” recipient will (1) hold PHI “confidentially,” (2) that PHI will only be used or “further disclosed” as “required by law” or for purpose for which it was disclosed, and (3) recipient will notify BA of any “breach of confidentiality”
REQUIRED: BA must amend PHI in DRS as directed or agreed by CE	

The Old BA Regime

- BAC Penalties
  - CE may be penalized if CE "knew of a pattern of activity or practice" of the BA "that constituted a material breach or violation" of the BAC, unless:
    - The CE took "reasonable steps to cure the breach or end the violation" and, "if such steps were unsuccessful:"
    - Terminated the BAC, if "feasible," or if not "feasible" reported the problem to DHHS
      - 45 CFR §.504(e)(1)(ii)
  - No jurisdiction to penalize BAs for BAC violation, or any HIPAA regulatory violation

The Old BA Regime

- BA Subcontractor/Agent Workaround
  - BAs don’t/can’t perform all functions and activities for/on behalf of CEs involving use or disclosure of PHI by themselves
  - BAs may also need to permit other parties to have access to, use, disclose PHI for BA’s own functions and activities
  - How to protect PHI when non-BAs must access and/or control it?

The Old BA Regime

- BA Subcontractor/Agent Workaround
  - BAC allows disclosure by BA:
    - ***For purposes of the CE***: Mandatory provisions requiring BA to ensure that “any agent, including a subcontractor” to which it provides PHI “agrees to implement reasonable and appropriate safeguards to maintain it, and “agrees to the same restrictions and conditions what apply to the BA” with respect to it
      - 45 CFR §§ 164.314(a)(2)(i)(B), .502(e)(2)(ii)(D)
    - ***For purposes of the BA***: Optional provisions allowing BA to disclose PHI for its own “proper management and administration” and to “carry out legal responsibilities,” if recipient provides “reasonable assurances” it will hold PHI “confidentially,” PHI will be used or further disclosed only as required by law or for purposes for which it was disclosed, and recipient will notify BA of any “breach of confidentiality”
      - 45 CFR § 164.504(e)(4)

The Old BA Regime

- BA Subcontractor/Agent Workaround
  - Implicit distinction?
    - "Subcontractor" is third party to which BA provides PHI for purpose of the CE
    - "Agent" is a third party to which BA provides PHI for purpose of the BA
      - Except, not all third parties used by BA for BA administration, management, legal responsibilities necessarily meet the legal definition of "agent"
      - This began to matter a lot under the Breach Notification Rules (2009), which provide that a breach is known to a CE or BA at the time it is known to its agent
    - Possible distinction never really analyzed or discussed in depth

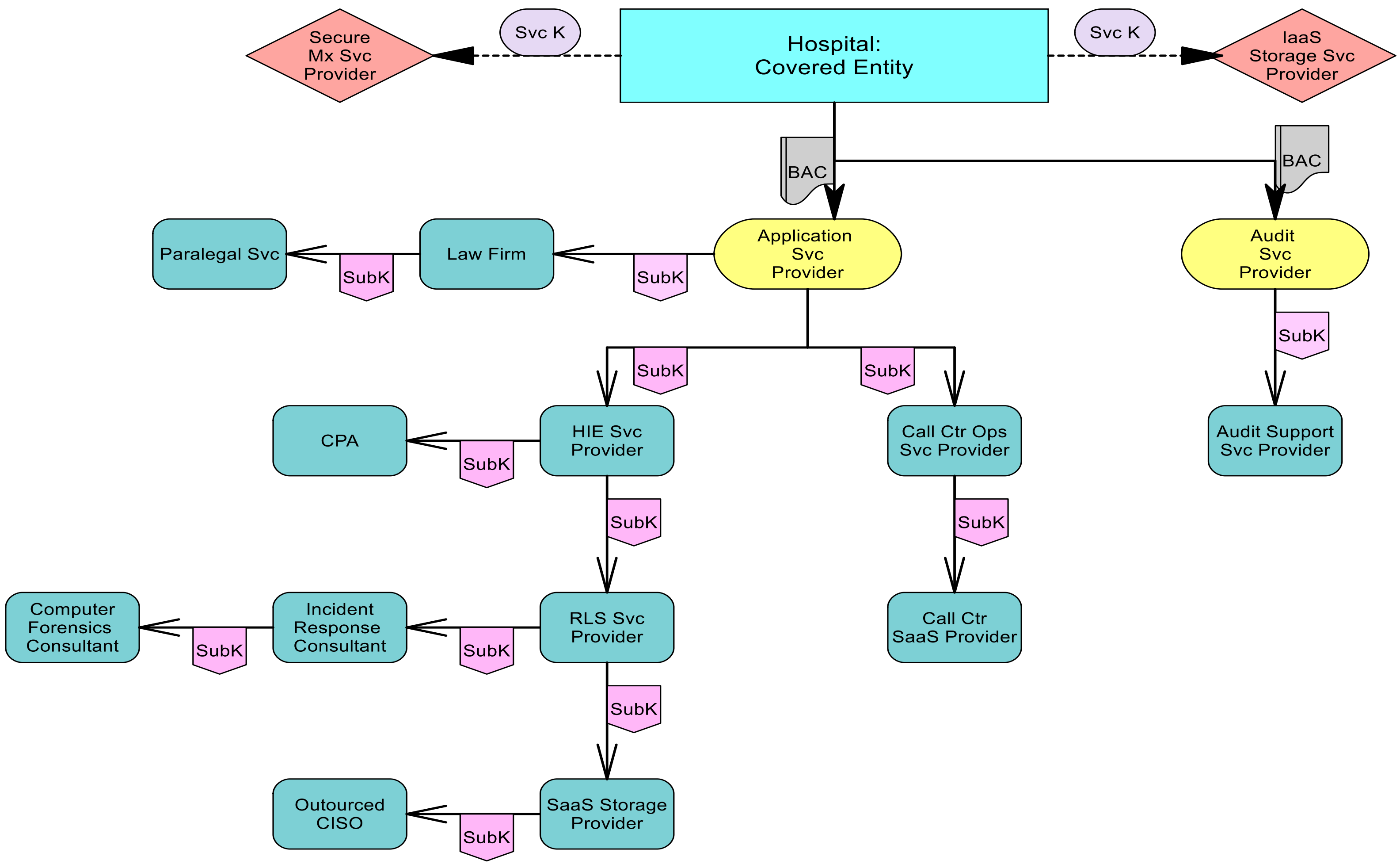
The Old BA Regime

- "Conduit" Concept
  - BA does not include data transmission services provider which does not require access to PHI, and in fact has only "random or infrequent" access to PHI
  - Explanatory interpretation, not regulation
  - Base analogy: Postal service
    - Information delivered in sealed envelopes
    - Envelopes not intended to be opened in transit
    - Legal prohibitions on opening envelopes in transit
    - Access may occur anyway by accident (torn envelope) or random/infrequent legal requirement (postal inspection under warrant)

The Old BA Regime

- “Conduit” Concept
  - In absence of detailed or supplemented explanation, some interpreted “conduit” concept as potentially applicable to data storage, where storage services provider did not require access to PHI, and in fact had only random/infrequent access
    - Some debate over whether stored PHI had to be encrypted, services provider could not have keys

The Old BA Regime



The Old BA Regime

- Hospital is sole CE on chart
- Application and audit services providers are only BAs
- Secure messaging and infrastructure-as-a-service (IaaS) storage services providers are conduits
- All other parties are subcontractors or agents (not distinguished)

The New BA Ecology

- HITECH Mandates
  - HITECH § 13401(a) mandates application of HIPAA Security Rule to BAs “in the same manner” as to CEs, requires that HITECH security requirements applicable to CEs apply to BAs, and requires that all such provisions “shall be incorporated” into the BAC
  - HITECH § 13404(a) mandates application of HIPAA BAC regulations (45 CFR § 164.504(e)) to BAs as regulatory requirements, requires that HITECH privacy requirements applicable to CEs apply to BAs, and requires that all such provisions “shall be incorporated” into the BAC.

The New BA Ecology

- Megarule BA Revision (45 CFR § 160.103)
- A "person" who is not a CE workforce member and:
  - "~~Performs or assists in the performance of" a function or activity involving the use or disclosure of PHI on behalf of a CE~~
    - ~~Official examples: Claims processing or administration; data analysis, processing or administration; utilization review; billing; quality assurance; benefit management; practice management, repricing~~
    - ~~Any other "function or activity " regulated under HIPAA~~
    - **"Creates, receives, maintains, or transmits PHI for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing;"**

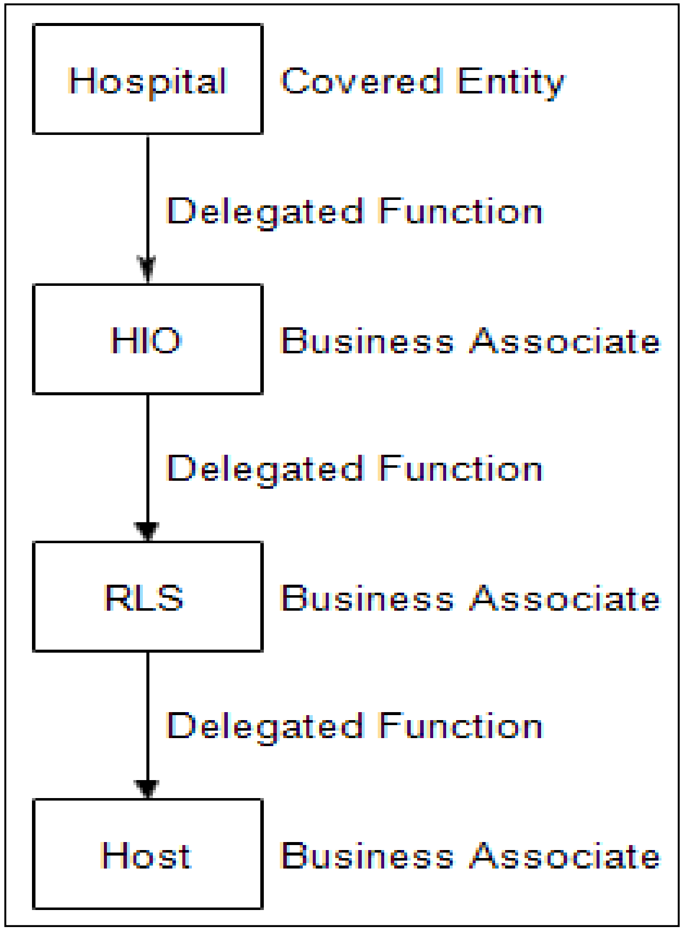
The New BA Ecology

- Megarule BA Revision (45 CFR § 160.103)
  - A “person” who is not a CE workforce member and:
    - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services on behalf of a CE, involving disclosure of PHI for purposes of the services to the BA by the CE or another BA
    - **A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a CE and that requires access on a routine basis to such PHI health information.**
    - **A person that offers a personal health record to one or more individuals on behalf of a CE.**
    - **A subcontractor that creates, receives, maintains, or transmits PHI on behalf of a BA**

The New BA Ecology

- New Subcontractor Definition (45 CFR § 160.103)
  - Subcontractor means a person to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA
    - If a BA delegates a function involving PHI to a subcontractor, that subcontractor becomes a BA
    - If the subcontractor/BA in turn delegates a function involving PHI to another subcontractor, that other subcontractor becomes a BA
    - And so on, as far as activities, functions and services involving PHI are delegated
  - A "chain of trust" for PHI

The New BA Ecology



- "Upstream:" CE, or BA delegating function
- "Downstream:" BA to which function is delegated
- "First tier" BA: BA with direct delegation from CE
- "Second tier" BA: BA with direct delegation from first tier BA (and third, fourth tier, etc.)
- "Lower tier" BAs: BAs below first tier

The New BA Ecology

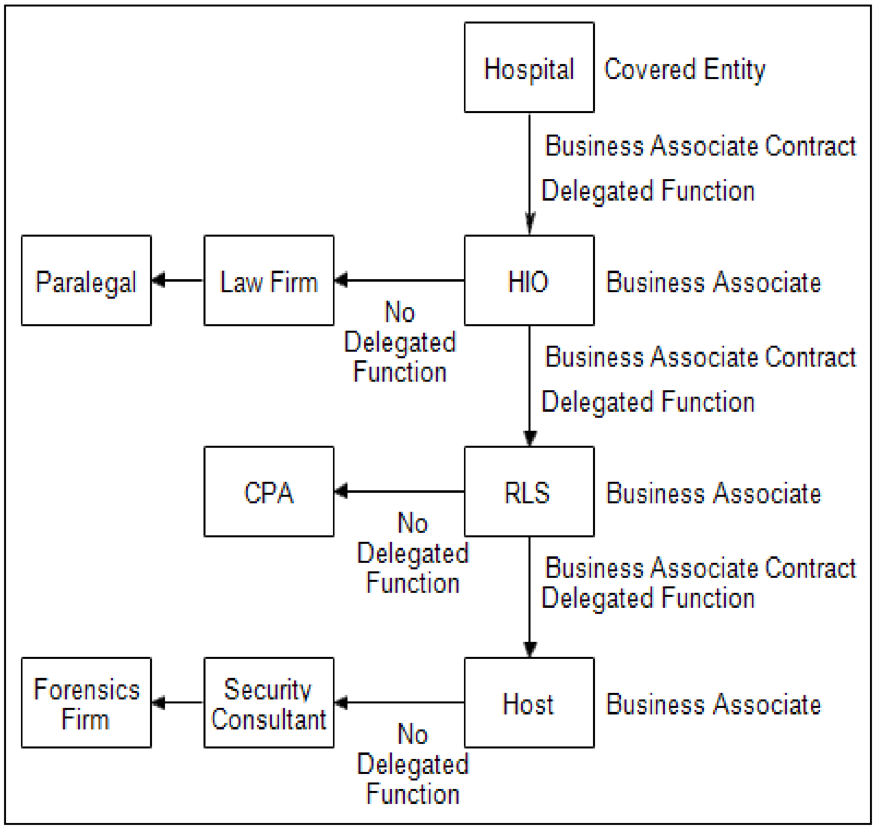
- Each Subcontractor is a fully regulated BA by definition
- CE is only required to have a BAC with the First Tier BA
- Each BA in the chain is required to have a BAC with its Subcontractor
- Each Upstream BA is only required to have a BAC with its immediate Downstream BA
- Same principles apply to governmental agencies (MOUs) and group health plans (plan documents and related contracts)

The New BA Ecology

- Subcontractor/BAs Do Not Include Recipients of PHI for BA Purposes
  - "We also provide the following in response to specific comments. Disclosures by a business associate pursuant to § 164.504(e)(4) and its business associate contract for its own management and administration or legal responsibilities do not create a business associate relationship with the recipient of the [PHI] because such disclosures are made outside of the entity's role as a business associate."
    - Preamble to Megarule at 5574
    - Not limited to "agents" of BA
    - Not a regulation, but an interpretation

  - Call it a "BA Services Provider?"

The New BA Ecology



- BA retains BA Services Provider to does not perform function, activity or service involving PHI for purposes of BA
- BA Services Provider may use, disclose PHI for BA purposes
- BA Services Provider may use other parties to provide support/related services for BA purposes
  – These parties are also not BAs

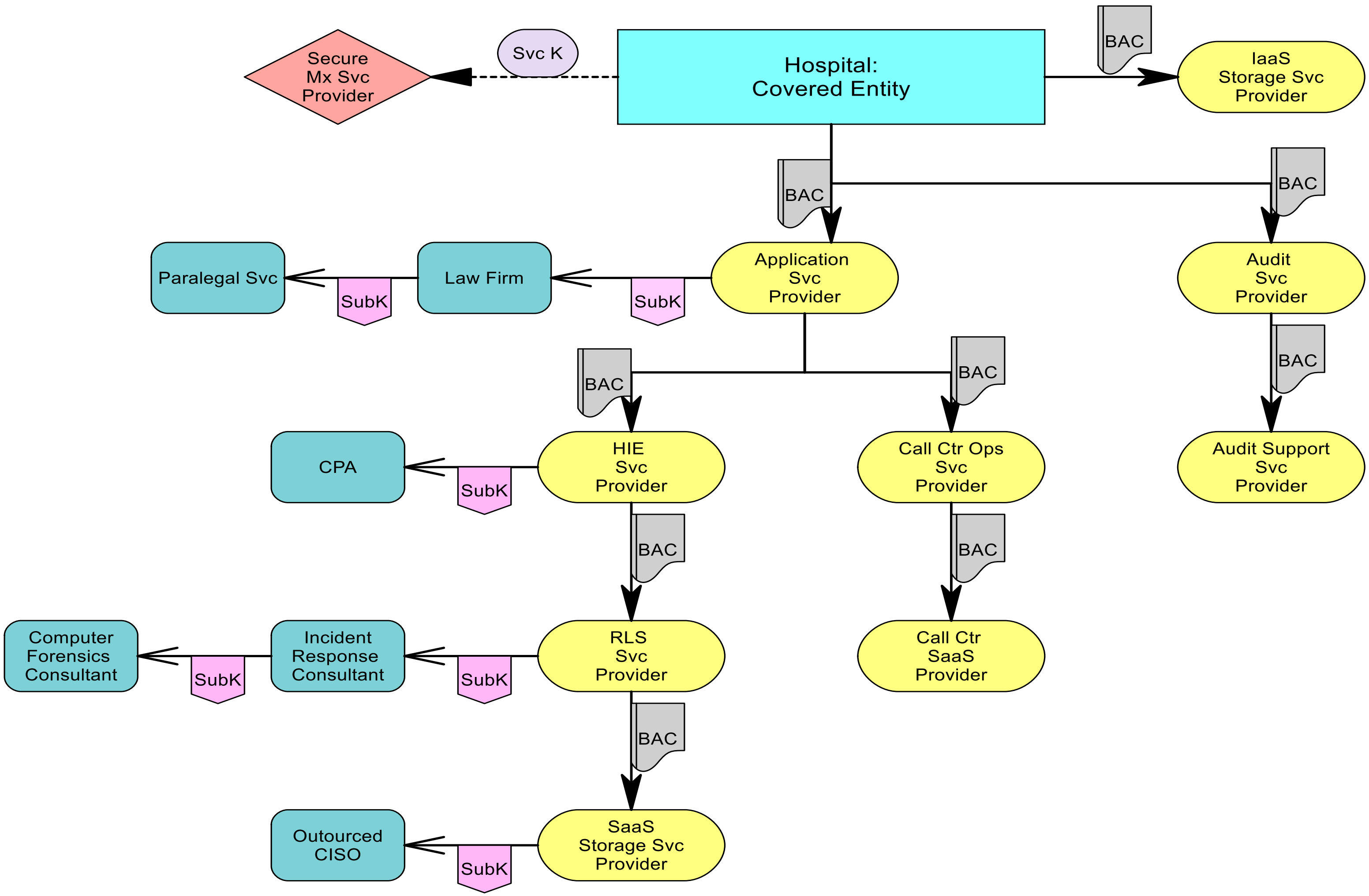
The New BA Ecology

- "Conduit" Exception Limited to Transmission Services Only
  - "The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services."
    - Preamble to Megarule at 5571
  - Not a regulation, but an interpretation

The New BA Ecology

- “Conduit” Exception Limited to Transmission Services Only
  - Webinar comments by OCR official indicate that electronic storage services provider which does not need to access PHI, does not do so on even a random or infrequent basis, and in fact cannot do so because PHI is encrypted and services provider does not have the encryption keys, is still a BA
    - Contrary to overall concept that BA status turns on “access” to PHI
    - In practice, storage services provider might not even know PHI was being stored – and so not know they were BA

The New BA Ecology



The New BA Ecology

- Hospital is still sole CE on chart
- Application services provider has two chains of downstream BAs
  - Each downstream BA has BA Services Provider; two have BA Services Provider chains
- Audit services provider has one downstream BA
- IaaS storage services provider is now a BA
- Messaging services provider is the only conduit

New BA Compliance Obligations

- Direct Regulatory Obligations
  - Full compliance with the Security Rule
  - Use and disclose PHI **only as permitted by the upstream BAC**
  - Comply with the Minimum Necessary rule
  - Notify **the CE** in case of a security breach
    - More discussion of BA breach notification to come
  - Provide access to a copy of the electronic PHI in their possession to the CE or individual, as specified in their upstream BAC
  - Provide the information needed for an accounting of disclosures
  - Provide access to their records to OCR to investigate the BA's compliance
  - Requirement for implementing BACs with any downstream BA
    - Belt and suspenders: Many BAC requirements are redundant to regulatory requirements

New BA Compliance Obligations

- BAC Requirements
  - BA must comply with Security Rule (redundant to regulation)
  - BA musts report security incidents and breaches (partially redundant)
  - BA must accept restrictions on use or disclosure of PHI in BAC (redundant)
  - BA must make PHI available to individuals (redundant)
  - BA must provide information for accounting of disclosures (redundant)
  - BA must make internal practices, books, etc. available to OCR (redundant)
  - BA must amend PHI upon request
  - If BA is carrying out CE Privacy Rule obligation, perform consistently with requirements for CE

New BA Compliance Obligations

HIPAA BAC Content	
REQUIRED: Define permitted uses and disclosures of PHI for purposes of underlying agreement	**REQUIRED:** BA must provide information needed for accounting of disclosures by CE
REQUIRED: No prohibited use or disclosure of PHI by BA	**REQUIRED:** BA must make internal books, records, etc. available to DHHS for determination of CE compliance
REQUIRED: BA must use "appropriate" safeguards to prevent use or disclosure of PHI other than as permitted by BAC or required by law	**REQUIRED:** BA must return or destroy all PHI upon termination of BAC, or may escrow if return or destruction not feasible
REQUIRED: BA must comply implement administrative, physical and technical safeguards to reasonable and appropriately protect confidentiality, integrity, availability of electronic PHI, **in compliance with the Security Rule**	**REQUIRED:** BAC must allow CE to terminate BAC for BA violation
	REQUIRED: To the extent the BA carries out CE responsibilities, BA must comply with CE regulatory obligations
REQUIRED: BA must report security incidents, **including breaches**, to CE or upstream BA as applicable	**OPTIONAL:** BA may use PHI, "if necessary," for BA's "proper management and administration"
REQUIRED: BA must ensure that any subcontractor ~~or agent~~ to which it provides PHI implements "reasonable and appropriate safeguards" to protect it	**OPTIONAL:** BA may use PHI, "if necessary," to "carry out the legal responsibilities of the BA"
REQUIRED: BA must ensure that any subcontractor or agent to which it provides PHI "agrees to the same conditions and restrictions that apply to the BA" under the BAC	**OPTIONAL:** BA may disclose PHI "if required by law"
REQUIRED: BA must make any PHI in designated record set (DRS) available for individual access	**OPTIONAL:** BA may disclose PHI to for BA's management, administration, legal responsibilities, upon "reasonable assurances" recipient will (1) hold PHI "confidentially," (2) that PHI will only be used or "further disclosed" as "required by law" or for purpose for which it was disclosed, and (3) recipient will notify BA of any "breach of confidentiality"
REQUIRED: BA must amend PHI in DRS as directed or agreed by CE	

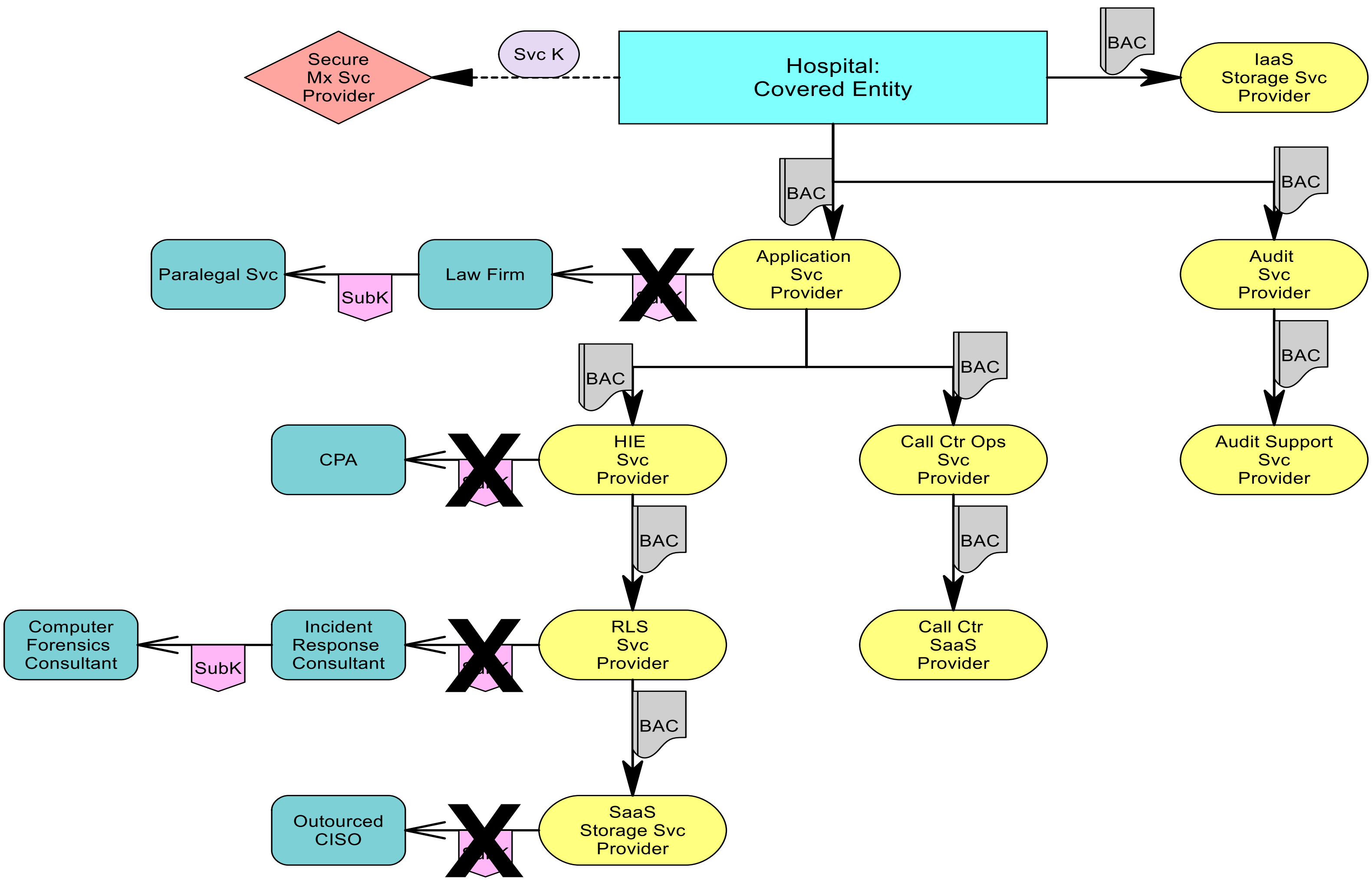
BA Chain Problems

- PHI Use and Disclosure Authorization
  - A BA may not authorize any use or disclosure of PHI not authorized by its upstream BAC
  - Authorization in downstream BAC must be equivalent to or more stringent than authorization in upstream BAC
  - Upstream BAC provisions should allow for legitimate optional uses and disclosures

BA Chain Problems

- PHI Use and Disclosure Authorization Sample Problem
  - HIO BAC with record locator service does not include optional provisions allowing disclosure of PHI to carry out legal responsibilities or proper management, or to BA Services Provider
    - RLS experiences security breach affecting PHI
    - Vendor is not authorized to retain law, security consulting or computer forensics firms to advise about, contain, mitigate and investigate breach, if services require possible access to PHI

BA Chain Problems



BA Chain Problems

- Pass-along of CE compliance obligations with delegated functions, activities
  - Example: Hospital outsources electronic health record (“EHR“) functions to application services provider
  - Hospital delegates provision of copies of records to individuals to vendor as part of EHR services
  - Vendor delegates health information management functions to HIM outsourcing firm
  - Outsourcing firm must be bound to 60 day turnaround, electronic format requirements applicable to provision of copies by hospital

BA Compliance Planning

- Compliance Timing and BACs
  - No “grandfathered” contracts as proposed
  - Some BACs “deemed compliant” until September 22, 2014
    - To be “deemed compliant” a BAC must be:
      - In compliance with pre-HITECH HIPAA BAC requirements
      - In effect before January 25, 2013,
      - Not apply to agreements or arrangements which are renewed (for evergreen contracts) or amended before September 23, 2013
        - » In other words, if the underlying agreement of a BAC is renewed or amended, the BAC is no longer deemed compliant, even if the BAC is not amended
    - “Deemed compliant” status terminates on the earlier of:
      - Renewal or amendment of the underlying agreement, or
      - September 22, 2014

BA Compliance Planning

- Transition Planning for CEs
  - Identify all BAs and BACs
    - Specify any where “deemed compliant” status may be desired
    - Rank according to upcoming renewal or anticipated amendment dates
  - Develop form(s) of HITECH-compliant BAC in preferred form
    - Possible variations for different types of BA, e.g. different types of services vendor, consultants, etc.
      - Chain considerations: Limitations, notification, due diligence on lower tier BAs?
      - Agents!

BA Compliance Planning

- Transition Planning for CEs
  - Consider pros and cons of non-required provisions, e.g. indemnification for breach response costs
  - Develop a plan for rolling out revised BACs
    - Anticipate some may need negotiation, some may involve a “battle of the forms” between BACs, some BAs may be partially or entirely without a clue

BA Compliance Planning

- Transition Management for BAs
  - Do Security, Breach Notification and Privacy Rule gap analysis ASAP
    - Revising or implementing fully compliant program by September 23 may be a challenge
  - Identify all Upstream CEs and BAs and Downstream BAs
    - If Lower Tier BA, identify CE at the top of the chain
    - Specify any where “deemed compliant” status may be desired
    - Rank according to upcoming renewal or anticipated amendment dates

BA Compliance Planning

- Transition Management for BAs
  - Review chain BACs
    - If BA is “middle tier” (has delegated functions, activities from upstream BAC to downstream BA), ensure downstream terms are consistent with upstream
  - Develop form(s) of HITECH-compliant BAC in preferred form
    - Possible variations for different types of BA, e.g. different types of services vendor, consultants, etc.
      - Chain considerations: Limitations, notification, due diligence on lower tier BAs
      - Agents!
    - Consider pros and cons of non-required provisions, especially breach notification

BA Compliance Planning

- Transition Management for BAs
  - Review existing BA Services Provider contracts
  - Develop form(s) of HITECH-appropriate BA Services Provider agreement in preferred form
    - BA Services Provider chain considerations: Limitations, notification, due diligence on subcontractors
    - Agents!
    - Consider pros and cons of non-required provisions, especially breach notification
  - Develop a plan for rolling out revised BACs and BA Services Provider agreements
    - Anticipate some may need negotiation, some may involve a “battle of the forms,” some CEs and/or BA Services Providers may be partially or entirely without a clue

Security Breaches

- Interim Final Rule Updated by Megarule
  - Breach is any "acquisition, access, use, or disclosure" of "unsecured PHI in a manner not permitted under" the Privacy Rule "which compromises the security or privacy" of the PHI
    - Change from the IFR, which defined breach as compromise of PHI which "poses a significant risk of financial, reputational, or other harm to the individual"
  - Breach does not include:
    - Good faith, unintentional acquisition by person otherwise authorized to access PHI, with no retention of information
    - Inadvertent disclosure by person authorized to access PHI with no further non-permitted use or disclosure
    - Disclosure to unauthorized person, where a CE or BA has a good faith belief that s/he would not reasonably have been able to retain such information

Security Breaches

- “Unsecured PHI” does not include PHI rendered “unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by” OCR

- Specified technologies and methodologies:
  - Encryption of “data at rest” consistent with NIST Special Publication 800–111, ***Guide to Storage Encryption Technologies for End User Devices***
  - Encryption of “data in transmission” consistent with Federal Information Processing Standards (FIPS) 140–2; NIST Special Publications 800–52, ***Guidelines for the Selection and Use of Transport Layer Security*** (TLS) Implementations; 800– 77, ***Guide to IPsec VPNs***; or 800–113, ***Guide to SSL VPN***

Security Breaches

- “Unsecured PHI” does not include PHI rendered “unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by” OCR

- Specified technologies and methodologies:
  - Media containing information has been:
    - If paper, film, or other hard copy, shredded or destroyed so information cannot be read or reconstructed
    - If electronic, has been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, ***Guidelines for Media Sanitization***

Security Breaches

- Interim Final Rule Updated by Megarule
  - Burden is now on CE or BA to demonstrate that there is a “low probability” that the PHI has been compromised “based on a risk assessment of least the following factors:
    - Nature and extent of the PHI involved, including types of identifiers and 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

Security Breaches

- Notification by CE and/or BA
  - If 500+ individuals, notify OCR and individuals “without unreasonable delay,” no more than 60 days from discovery, subject to law enforcement delay as requested by law enforcement
    - Must include notification via “prominent media outlets”
  - If 500 or fewer, notify individuals within 60 days, OCR within 60 days of end of calendar year in which breach occurs
  - Breach considered “discovered” when actually known or “by exercising reasonable diligence” would have been known to CE
    - Breaches known to workforce members, agents of CE deemed “known” to CE
  - BA must notify CE of breach upon “discovery,” under same terms as CE “discovery”
  - Who’s an “agent?”

Security Breaches

- Breach Response and Notification Coordination Issues
  - Timing of BA notification: If BA is “agent” of CE, breach is deemed “discovered” by CE upon “discovery” by BA
    - Either avoid making BA an agent, or hold BA to rapid notification to allow timely CE notification
    - Lower Tier BAs should never be considered CE’s BA
    - May still be desirable to have Lower Tiers notify rapidly to avoid excessive response delay

BA Breach Notification Problems

- CE Has the Obligation to Notify Individuals and OCR
  - "A CE shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the CE to have been, accessed, acquired, used, or disclosed as a result of such breach."
  - "A CE shall, following the discovery of a breach of unsecured PHI . . . notify [OCR]."
    - 45 CFR §§ 164.404(a), .408(a)

BA Breach Notification Problems

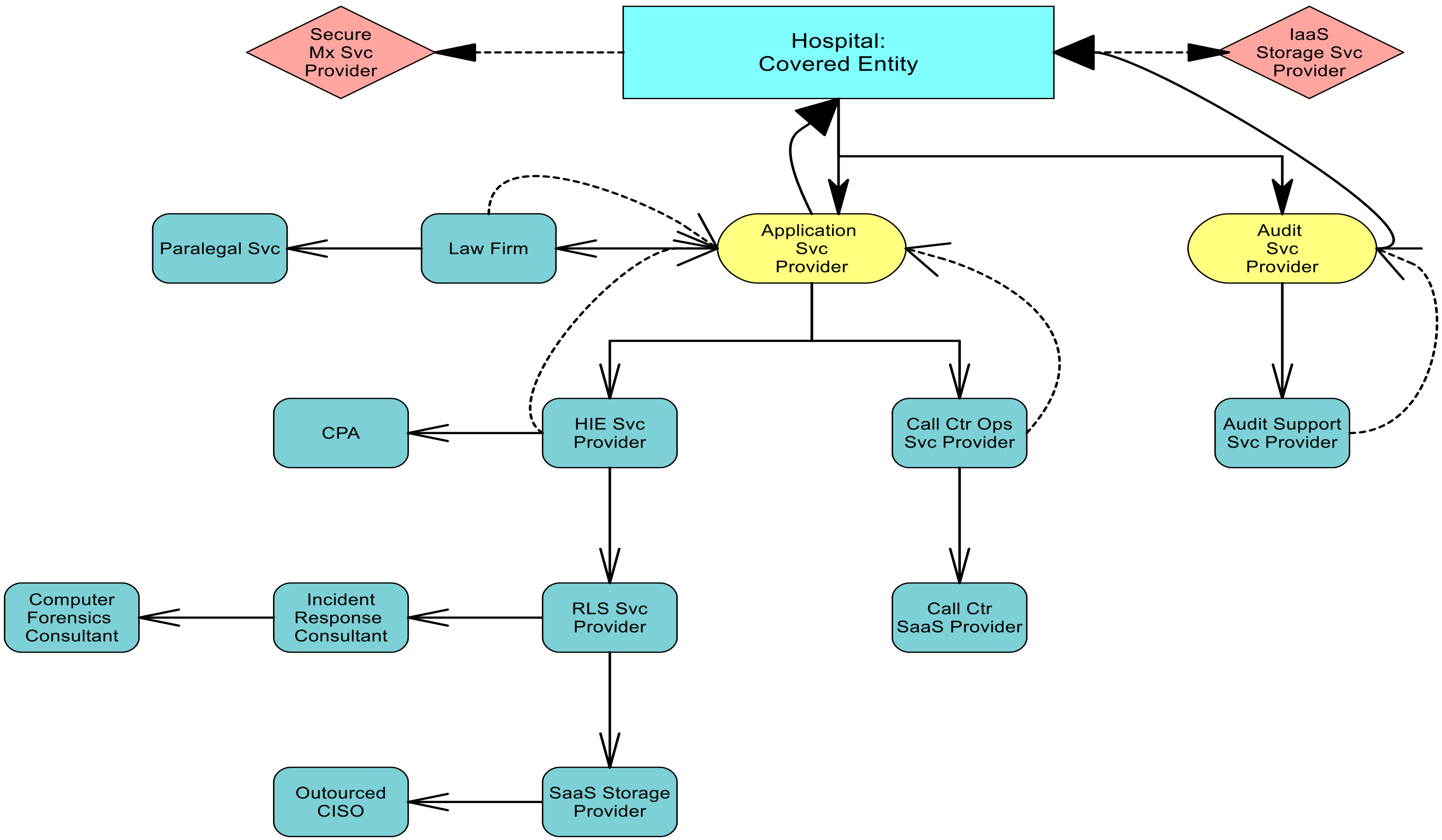
- Each BA in a Chain Has an Obligation to ***Notify the CE***
  - “A BA shall, following the discovery of a breach of unsecured PHI notify the CE of such breach.”
    - 45 CFR § 164.410(a)(1)
  - Required BAC provision that BA must “report to the CE any security incident of which it becomes aware, including breaches of unsecured PHI as required by § 164.410.”
    - 45 CFR § 164.314(a)(2)(i)(C)
  - CE may delegate notification to BA
    - Megarule at 5651.

BA Breach Notification Problems

- Each BA in a Chain Has an Obligation to ***Notify the CE***
  - No regulatory obligation for lower tier BAs to notify upstream BAs
    - Only applicable if provided for in non-required BAC provision
  - No regulatory obligation for BA Services Providers to notify CE
    - BA “assurances” from BA Services Providers must include notification of “breach of confidentiality”
    - Is that the same as a “breach” under the Breach Notification Rule?

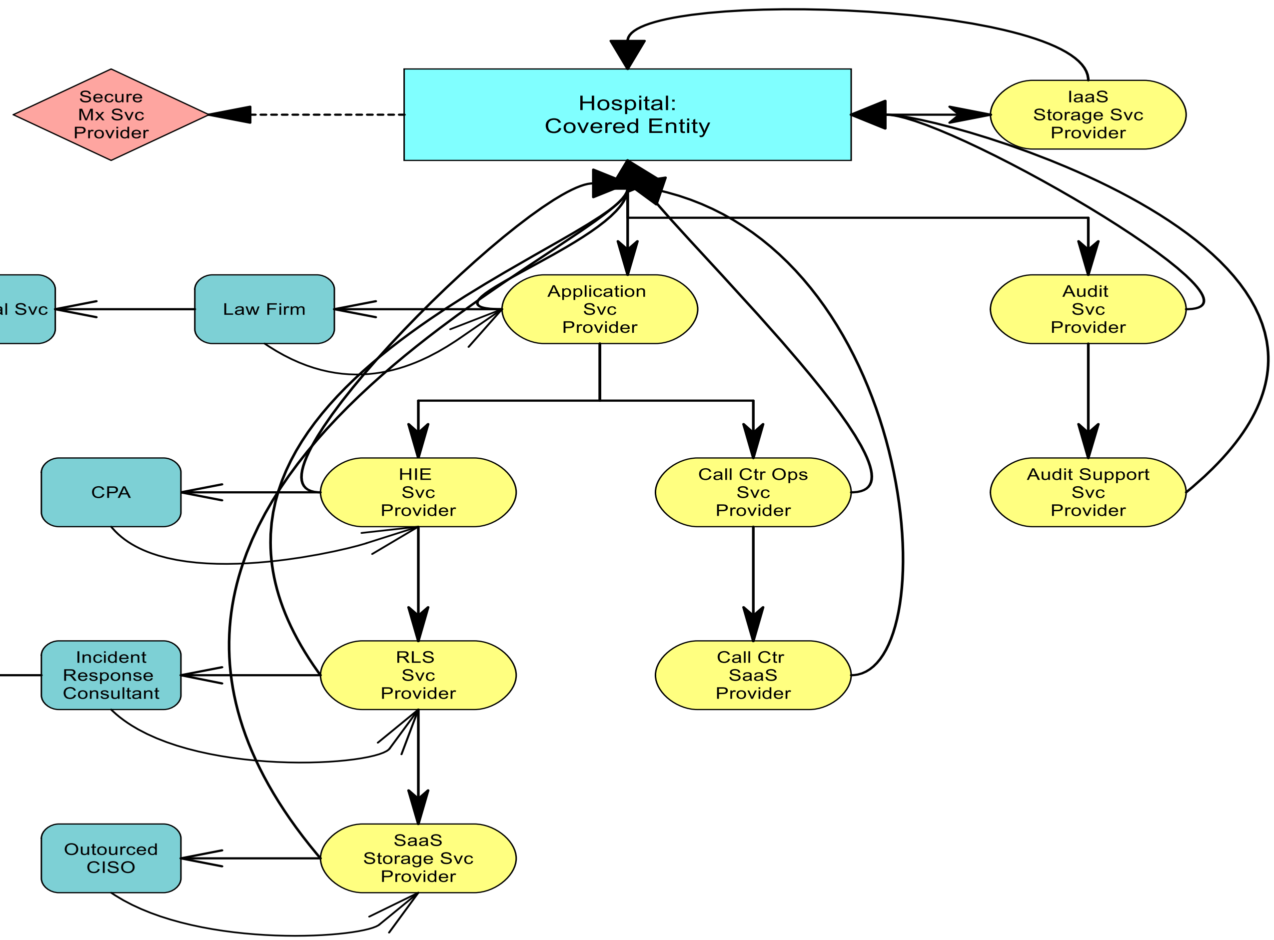
BA Breach Notification Problems

Pre-Megarule Notification by BAs



BA Breach Notification Problems

Post-Megarule Notification by BAs



BA Breach Notification Problems

- Who Determines If It's a "Breach?"
  - Any "acquisition, access, use, or disclosure of PHI in a manner not permitted under [the Privacy Rule] is presumed to be a breach **unless the CE or BA, as applicable**, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:"
    - Nature and extent of the PHI involved, including types of identifiers and 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
      - » 45 CFR § 164.402 (emphasis added)

BA Breach Notification Problems

- Timing of Notification by BA
  - BA must notify CE of breach upon its “discovery”
  - Breach considered “discovered” when actually known or “by exercising reasonable diligence” would have been known to BA
    - Breaches known to workforce members, agents of BA deemed “known” to BA
  - Breaches known to BA which is “agent” of CE deemed “known” to CE

- Who’s an “agent?”

BA Breach Notification Problems

- The Federal Common Law of Agency
  - Agent must have either actual or apparent authority, or the principal must ratify the agent's unauthorized actions.
  - Actual authority may be express or implied.
  - An agent has express authority when the principal explicitly grants the agent the authority to perform a particular act.
  - An agent has implied authority for the performance or transaction of anything reasonably necessary to effect execution of his express authority.
    - Implied authority is actual authority that is implied by facts and circumstances and it may be proved by circumstantial evidence. Only the words or conduct of the alleged principal, not the alleged agent, establish the authority of the agent.

BA Breach Notification Problems

- The Federal Common Law of Agency
  - Highly specific, fact-based question
    - Based on analysis of overall relationship between CE and BA, not just BAC
  - Control over assigned tasks; skill required; sources of the “instrumentalities and tools”; location of the work; duration of the relationship between the parties; right to assign additional projects; discretion over time, timing; method of payment; discretion over assistants; whether work is part of regular business of hiring party; whether hiring party is in business; provision of employee benefits; tax treatment
    - ERISA plan administrative committee found to be agent of plan sponsor employer. ***Woods v. Qwest Info. Tech***., 334 F. Supp. 2d 1187 (D. Neb. 2004)

BA Breach Notification Problems

- Breach Response and Notification Coordination Issues
  - Timing of BA notification to CE
    - 60 days if BA is not agent of CE
    - ASAP if BA is agent of CE, as breach is deemed “discovered” by CE upon “discovery” by BA, even if BA has not notified CE
      - Either avoid making BA an agent, or hold BA to rapid notification to allow timely CE notification
      - Lower tier BAs should never be considered CE’s BA
    - If lower tier BA is agent of upstream BA, is upstream BA deemed to have “discovered” breach when lower tier BA did?
      - What if upstream BA is in turn agent of the CE? When is the CE deemed to have “discovered” the breach?

BA Breach Notification Problems

- Breach Response and Notification Coordination Issues
  - State breach notification laws
    - State breach notification laws apply according to residency of individual, not location of breach, CE or BA
    - State authorities may require notification
    - Different notification standards may apply
    - BA may have independent notification requirements

BA Breach Notification Problems

- Breach Response and Notification Coordination Issues
  - Who pays notification costs?
    - Slightly under $20/record per recent studies
  - Investigation, remediation costs can be very high
  - Is indemnification under BAC really appropriate?
  - Is BA notification cost exposure proportionate to overall contract benefits?
  - Is insurance available?

BA Breach Notification Problems

- Summary of BA Notification Questions
  - Is the first tier BA an agent of the CE?
  - In a chain relationship, are any lower tier BAs agents of upstream BA?
    - Do they have BAC obligation to notify upstream BA?
  - Is any BA Services Provider agent of a BA?
    - What timing do they have for BA notification of breach?
  - How do lower tier BAs notify CE of security incidents and breaches?
    - Is upstream BA authorized to receive notices on behalf of CE?
  - Can/should a BA determine whether an incident constitutes a breach?
    - If it determines it is not, must still notify CE of an “incident”
    - Should CE delegate authority to BA to make determination?
  - What state notification laws apply?
    - What obligations do they impose on BAs?

Criminal Enforcement

- Criminal Penalties
- Criminal penalties may be imposed only upon proof beyond a reasonable doubt that a “person”:
  - Knowingly and
  - In violation of HIPAA or any of its regulations,
  - Either:
    - Uses “or causes to be used” a unique health identifier (as required by regulation, e.g. plan or provider number);
    - Obtains individually identifiable health information; or
    - Discloses individually identifiable health information to another person
      - 42 USC 1320d-6(a)

Criminal Enforcement

- Criminal Penalties
  - Three levels:
    - “Simple” offense (proof of all elements)
      - Fine of not more than $50,000, not more than one year imprisonment, or both
    - “False pretenses” offense (proof of all elements, ***plus*** proof offense committed “under false pretenses”
      - Fine of not more than $100,000, not more than five years imprisonment, or both
    - “Bad intent” offense (proof of all elements, ***plus*** proof of “intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm”)
      - Fine of not more than $250,000, not more than ten years imprisonment, or both
      - 42 USC 1320d-6(b)

Criminal Enforcement

- Criminal Penalties
  - Proving the elements of the offense
    - "Knowingly:" Knowledge of facts indicating the existence of a violation, including actual and circumstantial knowledge, and failure to inquire where circumstances are suspicious
    - "In violation of" HIPAA provision: Must be required to comply as of time of offense
    - "Obtains" information: Includes any exercise of control, direct or indirect
      - Example: Supervisor instructs subordinate to copy information
    - "Disclose" information: Any "release, transfer, provision of access to or divulging in any other manner"

Criminal Enforcement

- Several Prosecutions to Date
  - U.S. v. Holland, Miller and Griffin (2011)
    - Doctor and two hospital employees snooped in celebrity patient file
    - Doctor sentenced to one year probation, $50,000 fine, 50 hours community service educating professionals about HIPAA. Other employees sentenced to one year probation, $1,500 and $2,500 fine respectively.
  - U.S. v. Zhou (2010)
    - Terminated physician snooped in co-workers', other patients medical records
    - Four months in prison
  - U.S. v. Smith (2008)
    - Clinic nurse gave PHI to husband who used it to threaten data subject
    - Two years probation, community service
  - U.S. v. Gibson (2004)
    - Phlebotomist at Seattle Cancer Care Alliance used PHI to obtain credit cards in patient's name

Civil Enforcement

- Basic Principles
  - OCR to “seek cooperation” in “obtaining compliance”
  - OCR “may” provide “technical assistance” to assist with voluntary compliance
  - CEs and BAs must “keep such records” and submit “such compliance reports” as OCR determines necessary to determine compliance
  - CEs must cooperate with OCR investigations and permit access (during “normal business hours”) books and records, etc.
  - If requested information is in possession of another who refuses to cooperate, certify efforts to OCR

Civil Enforcement

- Initiation of Compliance Investigation
  - Any “person who believes a [CE or BA] is not complying with the administrative simplification regulations” may file a complaint with HHS
    - Every complaint is reviewed and the allegations are analyzed for compliance implications. – Susan McAndrew, OCR Deputy Director
  - OCR may conduct “compliance reviews” on own initiative
  - OCR required to investigate where facts indicate possible “willful neglect”
    - “Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.”
  - May be triggered by security breach notification
    - Every breach involving more than 500 individuals is reviewed for privacy and security compliance. - Susan McAndrew

Civil Enforcement

- Basic Principles
  - OCR to “seek cooperation” in “obtaining compliance”
  - OCR “may” provide “technical assistance” to assist with voluntary compliance
  - CEs and BAs must “keep such records” and submit “such compliance reports” as OCR determines necessary to determine compliance
  - CEs must cooperate with OCR investigations and permit access (during “normal business hours”) books and records, etc.
  - If requested information is in possession of another who refuses to cooperate, certify efforts to OCR

Civil Enforcement

- Initiation of Compliance Investigation
  - Any “person who believes a [CE or BA] is not complying with the administrative simplification regulations” may file a complaint with HHS
    - Every complaint is reviewed and the allegations are analyzed for compliance implications. – Susan McAndrew, OCR Deputy Director
  - OCR may conduct “compliance reviews” on own initiative
  - OCR required to investigate where facts indicate possible “willful neglect”
    - “Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.”
  - May be triggered by security breach notification
    - Every breach involving more than 500 individuals is reviewed for privacy and security compliance. - Susan McAndrew

Civil Enforcement

- Initiation of Compliance Investigation
  - HITECH requires OCR to provide for “periodic audits” of compliance by CEs and BAs
  - HITECH requires OCR to “formally investigate” a complaint if “preliminary investigation of the facts . . . indicate[s] . . . a possible violation due to willful neglect”
  - State attorneys general granted civil penalties jurisdiction – and attorneys fees for successful action
    - Requires notice to OCR and opportunity to assume jurisdiction
    - OCR has provided training to state AG staff
  - Investigations may result in “resolution agreements,” including payment of non-penalty “resolution amount”
    - Providence Health & Services, $100,000
    - CVS, $2.25 million

Civil Enforcement

- Penalty Proceedings
  - If informal resolution not “satisfactory,” OCR to notify CE in writing. Burden on CE to satisfy OCR. If not satisfied, OCR may issue notice of proposed determination of civil monetary penalties
  - Notice to include findings of fact which are penalty basis
  - Target must pursue administrative appeal, through administrative law judge and internal DHHS Board of Appeals, before lawsuit

Civil Enforcement

- Privacy Rule enforcement from April 2003 (start of enforcement) through April 30, 2012:
  - Over 70,107 complaints
    - 39,283 not eligible for enforcement (no jurisdiction, etc.)
    - 16,105 resolved with corrective action plans
    - 8,310 finding no violation

- Security Rule enforcement from October 2009 (start of enforcement reporting) through March 31, 2012:
  - 559 complaints
    - 377 resolved with corrective action plans
    - 257 still pending

Civil Monetary Penalties

- HITECH requires CMPs and monetary settlements to be used by OCR for enforcement or distribution to affected individuals
- Distributions to “individuals harmed” by a violation to be determined by rule per methodology to be established by GAO
  - GAO report due August 2010, status unknown
  - Distribution rule due February 2012, status unknown (not included in Megarule)

Civil Monetary Penalties

- Pre-HITECH
  - Civil monetary penalty (CMP) maximum is $100/violation, to calendar year (Jan. 1 – Dec. 31) $25,000 maximum for “all violations of an identical requirement or prohibition”
- Core Concepts:
  - Single acts/events can implicate multiple requirements or prohibitions
  - Continuing violations – “a requirement or prohibition that is of an ongoing nature” – are counted at one per day of continuation

Civil Monetary Penalties

HITECH Penalties

Table 1 – Categories of Violations and Respective Penalty Amounts Available		
Violation Category – Section 1167(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	\$100 - \$50,000	\$1,500,000
(B) Reasonable Cause	\$1,000 - \$50,000	\$1,500,000
(C) Willful Neglect - Corrected	\$10,000 - \$50,000	\$1,500,000
(D) Willful Neglect - Corrected	\$50,000	\$1,500,000

Civil Monetary Penalties

- Penalty Determination
  - Affirmative defenses: Violation due to “reasonable cause,” not “willful neglect,” and under correction
  - Penalty aggravation/mitigation factors: Nature, harm caused by violation; intentional violation vs. violation “beyond control;” compliance history; financial factors

Civil Monetary Penalties

- *Reasonable cause* means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.
- *Reasonable diligence* means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.
- *Willful neglect* means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

Civil Monetary Penalties

- Example 1: Unauthorized access
  - BA allows unauthorized employee to access PHI on 20 individuals in [single?] computer file
  - BA has separate obligation to each individual
  - Unauthorized access to PHI of 20 individuals = 20 violations
  - If BA could not have known about this violation in the exercise of due diligence (unlikely?): $100/violation = $2,000 penalty
  - If BA permitted this due to reasonable cause (what would that be?): $1,000/violation = $20,000 penalty
  - If BA permitted this due to willful neglect (attended this seminar but failed to implement): $500,000/violation = $1.5 million penalty ($10 million, capped)

Civil Monetary Penalties

- Example 1 continued: Unauthorized access constitutes security breach
  - Unauthorized access is discovered during OCR investigation of unrelated complaint two years after event
  - BA failed to notify 20 affected individuals for two years
    - One or 20 separate continuing violations? 730 violations (2 x 360) or 14,600 violations (2 x 365 x 20)
  - BA failed to notify OCR within 60 days of end of calendar year of breach
    - One continuing violation for ten months: 300 violations
  - "Could not have known:" Probably not acceptable
  - "Reasonable cause:" Probably not acceptable
  - Willful neglect, not corrected: $500,000/violation
    - $3 million penalty
      - 730 x $500,00 = $3.65 **b**illion, capped at $1.5 million
      - 300 x $500,000 = $1.5 **b**illion, capped at $1.5 million

Civil Monetary Penalties

- Example 2: Defective business associate contract
  - CE enters into five business associate contracts authorizing PHI uses not permitted by Privacy Rule and not including required safeguards provision
  - 5 violations each of 2 separate provisions = 10 violations
  - If CE could not have known about this violation in the exercise of due diligence (probably not acceptable): $100/violation = $1,000 penalty
  - If CE permitted this due to reasonable cause (what would that be?): $1,000/violation = $10,000 penalty
  - Probably would be held CE permitted this due to willful neglect: $500,000/violation = $1.5 million penalty
    - 10 x $500,000 = $5 million, capped at $1.5 million

Civil Monetary Penalties

- Example 3: Negligent disposal of media
  - CE re-sells 100 used computers without scrubbing hard drives containing PHI on 1,000 individuals.
  - Potential violations:
    - Security Rule media re-use specification (100 violations)
    - Privacy Rule “little security rule” safeguards specification (1,000 violations)
    - Security Rule information access management standard (100 or 1,000 violations?)
    - Privacy Rule prohibited PHI use standard (1,000 violations)
    - Probably also presumed security breach if PHI was not properly encrypted

Civil Monetary Penalties

- Example 3 continued: Negligent disposal of media
  - Security Rule media re-use specification (100 violations)
    - Didn't know: $10,000
    - Reasonable cause: $100,000
    - Willful neglect: $1.5 million ($50 million, capped)
  - Privacy Rule "little security rule" specification (1,000 violations)
    - Didn't know: $25,000 ($100,000, capped)
    - Reasonable cause: $100,000 ($1 million, capped)
    - Willful neglect: $1.5 million ($500 million, capped)
  - Security Rule information access management standard (100 or 1,000 violations? – assume 100)
    - Didn't know: $10,000 ($100,000, capped)
    - Reasonable cause: $100,000 ($1 million, capped)
    - Willful neglect: $1.5 million ($50 million, capped)

Civil Monetary Penalties

- Example 3 continued: Negligent disposal of media
  - Privacy Rule prohibited PHI use standard (1,000 violations)
    - Didn't know: $25,000 ($100,000, capped)
    - Reasonable cause: $100,000 ($1 million, capped)
    - Willful neglect: $1.5 million ($500 million, capped)
  - Security Breach Notification Rule notification requirements
    - Didn't know: $25,000 ($100,000, capped)
    - Reasonable cause: $100,000 ($1 million, capped)
    - Willful neglect: $1.5 million ($500 million, capped)
  - Total
    - Didn't know: $95,000
    - Reasonable cause: $500,000
    - Willful neglect: $7.5 million

Civil Monetary Penalties

- Avoiding Penalties
  - Well-managed compliance program
  - Accountable program management
  - Policies and Procedures
  - Training and awareness
  - Internal auditing, testing and reporting
  - Services provider due diligence, tight contracting, oversight
  - Readiness to respond to security incidents and breaches
  - Readiness to respond to regulatory inquiries

Questions? Thanks!