EHR Contracting and Data Security

Briar Andresen

Steven Helland

January 10, 2018

Fredrikson & BYRON, P.A.

Overview

- What is required
- HIPAA-related issues
- Selecting a vendor
- Key provisions
  - Main EHR vendor
  - EHR adjacent
- Data security risks

© 2018 Fredrikson & Byron, P.A.

What is required?

- What are the “must-haves” for EHRs?
- Use certified EHR technology (CEHRT)

© 2018 Fredrikson & Byron, P.A.

What is required?

- For EHR incentive programs:
  - Eligible professionals, eligible hospitals, CAHs that participate in EHR Incentive Programs must show they haven't restricted compatibility or interoperability of certified EHRs
  - "Prevention of Information Blocking Attestation"
  - Don't have to show any documentation in order to attest
  - Continue to submit evidence of meaningful use to avoid payment reduction from Medicare or get incentive from Medicaid

© 2018 Fredrikson & Byron, P.A.

Donations of EHR

- Still ok (until Dec. 31, 2021, then?)
- Anti-kickback safe harbor, Stark exception
- Complex regulations; if you will provide or receive EHR function at less than FMV, review requirements carefully

© 2018 Fredrikson & Byron, P.A.

HIPAA and EHR contracting

- Patient's rights obligations
  - Amendment, access, requested restrictions
  - If a person requests electronic copy of PHI, must provide access in form/format requested, if readily producible
  - Images and other data must be included in electronic copy
  - Can you capture everything, and is there a process to do so?
    - Phone notes, provider notes, etc.
- Transition of records to a new vendor is a HIPAA issue

© 2018 Fredrikson & Byron, P.A.

HIPAA and EHR contracting

- Execute a BAA with the vendor
  - If they create, maintain (including in the cloud), receive, or transmit PHI
  - If they will have access (including for troubleshooting)
  - Indemnification in BAA for breaches (not just notification costs)
- Transition issues

© 2018 Fredrikson & Byron, P.A.

HIPAA and EHR contracting

- Make sure that, regardless of BAA status of the vendor, **new technology** is a part of an updated risk assessment
  - Risk assessment is ongoing, not once a year
    - If technology changes the EHR environment, it should affect the risk assessment
    - True for updates/upgrades, too
- Will information be transferred to vendor? How?
- Will vendor access EHR? What access is permitted?

© 2018 Fredrikson & Byron, P.A.

Risk assessment

- **Vendor** risk assessment before contracting
  - Access
  - Use
  - Review of policies and procedures?
  - Use outside of US?
- Is vendor willing to provide information about processes? Does it make sense?

© 2018 Fredrikson & Byron, P.A.

Selecting your EHR vendor

- Selection committee
- What are your functional requirements?
- What are your technical requirements?
- Pricing
- “Cloud” or “SaaS” vs. installed software
- RFPs or Proposals?
- Tip: Select at least 2 finalists

© 2018 Fredrikson & Byron, P.A.

Elements of an EHR contract

- **Quote/Proposal** with pricing, modules and schedule
- **License** or service **Terms and Conditions**
- **Maintenance and Support** terms and conditions
- **Statement of Work** outlining implementation, conversion, customizations, training, etc.
- **Service Level Agreement**
- **Business Associate Agreement**

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Pricing & Power of the Purse

  - Tie upfront payments to milestones and hold a portion until after Go Live
  - Annual/monthly fees start on Go Live, not contract signing
  - Cap the annual increases to maintenance or subscription

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Pricing continued
  - Counting. How are fees calculated? Pay attention to definition of “user,” “transaction,” “claims,” etc.
    - Tip: Sneaky terms may be hidden in “Definitions”
  - Ask about future pricing for additional users, new locations, new modules
  - Credit for acquisitions
  - Ability to reduce for divestitures

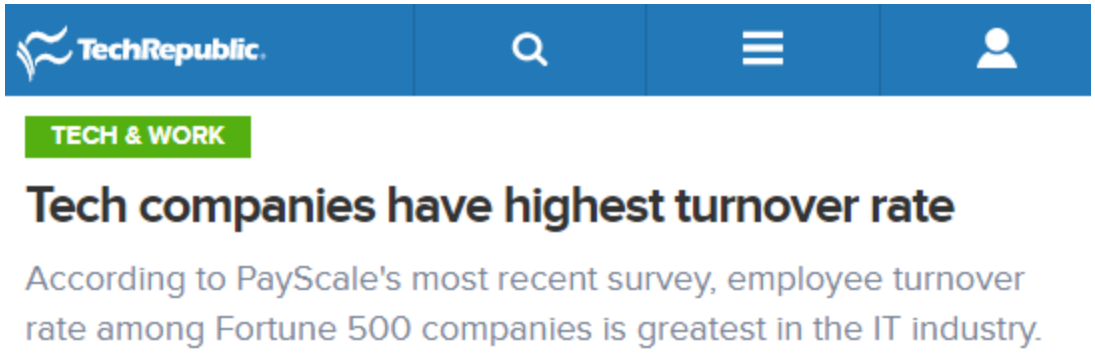
© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Implementation and acceptance testing
  - Portion of implementation and license fee should be tied to acceptance
  - Does the customer have a meaningful opportunity to confirm the functionality before Go Live?
  - "Failure to Launch": If vendor cannot correct deficiency, does customer have right to terminate for a full refund?
  - Contract term: Interoperability, required operating environment?

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts


TechRepublic

TECH & WORK

Tech companies have highest turnover rate

According to PayScale's most recent survey, employee turnover rate among Fortune 500 companies is greatest in the IT industry.

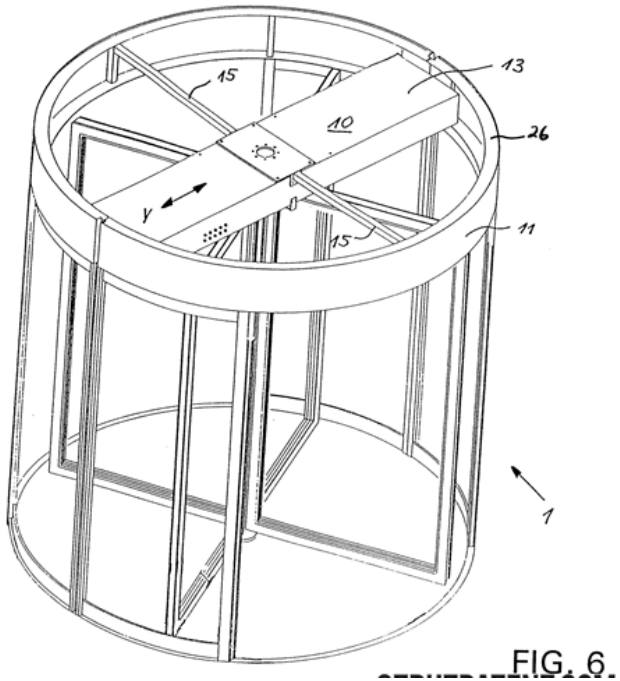


FIG. 6.

- Key personnel
  - Consistency
  - Right to remove
- Expenses / Travel costs
  - Warning: Can be 15-25% of implementation fees

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Term/Termination/Transition
  - For cloud-based software:
    - Annual or monthly renewals
    - Termination by customer for convenience at any time
  - For installed software:
    - perpetual software license with annual/monthly maintenance
    - Support and maintenance can be terminated by customer at any time or annually

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- No Plan to Sunset
  - Plan to continue to support, 5-7 years
  - Right to transition at no fee to successor product

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Warranties
  - Perform per “Documentation”
    - Tip: Plain English, and real examples.
  - Comply with laws and regulations
  - Non-infringement
  - Services will be provided in a professional and workmanlike manner
  - Vendor will diligently work with third party database vendors

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Limitation of Liability
  - Mutual (to fees paid)
  - No limit on vendor's liability for
    - Vendor's breach of BAA or other HIPPA violations
    - Security/confidentiality breaches
      - Tip: Stipulate, security breach liability includes cost of notice and 2 years credit monitoring.
    - Indemnification obligations
    - Fraud, gross negligence, intentional misconduct

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Indemnification from Vendor
  - intellectual property infringement
  - breach of privacy and security
  - Breach of warranties (maybe)
- Insurance
  - General liability
  - Worker's compensation
  - Employer's liability
  - Professional liability
  - Cyber / privacy

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Data privacy and security
- Particularly important in SaaS / Cloud
  - Documented security policies, standards and procedures
  - Physical security
  - Security audits / testing
- Backup obligations
- Disaster recovery

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Support and maintenance
  - Updates and other enhancements included in support fees
- Service levels
  - System up-time and response time
  - Support response and resolution time
  - Credits for failure
  - Ability to terminate for repeated SLA failures

© 2018 Fredrikson & Byron, P.A.

Key provisions in health IT contracts

- Jointly developed databases—who owns, who can use?
  - Can another vendor access that database? View it?

© 2018 Fredrikson & Byron, P.A.

Data security

- Who is helping you keep your data secure?
  - IT
  - Dedicated outside security vendor?
  - Vendors generally?
  - Employees—the front line
- When contracting, who reviews vendor access to PHI/the EHR?
  - Are firewalls in place?
  - Are minimum necessary requirements being met?

© 2018 Fredrikson & Byron, P.A.

Current events

© 2018 Fredrikson & Byron, P.A.

Scary health care issues: Phishing

KALAMAZOO NEWS

Phishing scam targeting hospital leaves 8,256 potentially exposed

Updated Jan 5; Posted Jan 5

10 93 shares

By **Al Jones**, ajones5@mlive.com

KALAMAZOO, MI - Bronson Healthcare Group says its email system was the target of an internet attack that potentially exposed information on several thousand patients.

The breach of email accounts of five employees potentially exposed information on 8,256 patients, but the medical records of those patients and others were never at risk, Bronson officials said.

© 2018 Fredrikson & Byron, P.A.

Scary health care issues: Ransomware

A Hospital Paralyzed by Hackers

A cyberattack in Los Angeles has left doctors locked out of patient records for more than a week. Unless the medical facility pays a ransom, it's unclear that they'll get that information back.

KAVEH WADDELL | FEB 17, 2016 | TECHNOLOGY

Share Tweet ...

TEXT SIZE − +

Like *The Atlantic*? Subscribe to The Atlantic Daily, our free weekday email newsletter.

Email SIGN UP

A hospital in Los Angeles has been operating without access to email or electronic health records for more than a week, after hackers took over its computer systems and demanded millions of dollars in ransom to return it.

The hackers that broke into the Hollywood Presbyterian Medical Center's servers are asking for $3.6 million in Bitcoin, a local Fox News affiliate reported. Hospital staff are working with investigators from the Los Angeles Police Department and the FBI to find the intruders' identities.

© 2018 Fredrikson & Byron, P.A.

Information blocking

- Deploying products with limited interoperability
- High costs for information exchange
- 21st Century Cures Act
  - Mandate for vendors and providers
- HIPAA BAA provisions

© 2018 Fredrikson & Byron, P.A.

Can you protect yourself?

- Educate employees
- Test (fake phishing emails)
- Have a plan if/when disaster strikes
  - What's the response? Who's in charge?
  - Have a potential cyber security partner to review situation, determine what information was compromised?
- Update anti-malware tools that can "predict" malware
- Patch on time!

© 2018 Fredrikson & Byron, P.A.

Can you protect yourself?

- No personal webmail on corporate-connected devices?
- Data backups (for long period of time)
- Maybe end up just paying….
- Look at options that make sense for your organization.
  - You can't guarantee complete protection, but you can make sure you are taking reasonable steps

© 2018 Fredrikson & Byron, P.A.

Contact information

Briar Andresen

612.492.7057

bandresen@fredlaw.com

Steve Helland

612.492.7113

shelland@fredlaw.com

© 2018 Fredrikson & Byron, P.A.