



Security and Privacy Issues in Connection with Wireless Technologies

Maryland HIMSS
Steven J. Fox, Esq.
October 31, 2008

Expanding Industry

- Wireless technology is rapidly expanding in the health care industry. It encompasses:
 - Networks (e.g., WLANs)
 - PDA's (e.g., personal devices for physicians, data collection and EHR-synced devices, personal fitness-related devices)
 - Call/communication devices (e.g., Vocera and IBM devices)
 - Medical devices (e.g., implanted devices transmitting physiological data)

© 2008 Steven J. Fox



Expanding Industry

- *Wireless Healthcare 2008* Report: Even amid recession, wireless health care technology is still a "buoyant" industry
 - By 2010, 80% of hospitals will have a wireless network
 - Investment of close to \$10B over the next 5 years
 - Significant cost-savings technology
 - Improved quality control and delivery processes

© 2008 Steven J. Fox



Challenges

- Network performance
 - Dell/Intel/Motion Computing launched new service to assess reliability of hospital's wireless network
- Battery life
- Physicians lacking confidence in applications (and continue using pen & paper)
- Compliance
 - Data Privacy standards; HIPAA
- Data Privacy and Security Breaches

© 2008 Steven J. Fox



Risks

- Rogue Access Points
 - failure to conform to security policy or left unsecured
- Hardware
 - factory defaults; improper configuration
- Sniffing
 - failure to use encryption
- Identity Theft
 - network's MAC address, not individual patients

© 2008 Steven J. Fox



Data Privacy and Security Compliance

- Data contained or transmitted via wireless networks or devices is subject to regulation by:
 - Federal legislation regarding PHI (Protected Health Information, e.g., HIPAA)
 - Applicable state legislation (e.g., record retention regulations)
 - Private associations (e.g., professional rules and guidelines)
 - Private contracts (e.g., Payment Card Industry Data Security Standards; applicable confidentiality and data privacy provisions in license or services agreements)

© 2008 Steven J. Fox



Data Privacy & Security Breaches

- 2008 saw numerous instances of major security breaches and ePHI loss, across all geographical regions and all major components of the healthcare industry. Examples include:
 - Horizon BC/BS (laptop; 300K affected)
 - Lifeblood (TN) (laptop; 300K+ affected)
 - HealthNet Federal Services (security breach; 100K+ affected)
 - BC/BS of Western New York (laptop; 40K affected)
 - Dental Network (NH) (web site security breach; 75K affected)
 - WellPoint (IN) (security breach; 120K+ affected)
 - WellCare Health Plans (GA) (security breach; 71K affected)
 - Staten Island University Hospital (security breach; 88K affected)
 - University of Utah Hospitals and Clinics (stolen tapes containing billing information; 2.2 million affected)
 - Florida Agency for Healthcare Administration (security breach; 55K affected)

© 2008 Steven J. Fox



Data Privacy & Security Breaches

- Health Care providers affected by data breaches and ePHI loss affecting less than 10,000 persons include large and small entities from all over the country, including:
 - HealthNet (stolen laptop; 5,000 affected)
 - Fallon Community Health Plan (stolen computer; 4,000 affected)
 - Wake County Emergency Services (laptop; 5,000+ affected)
 - University of MN (flash drive; 3100 affected)
 - Memorial Hospital, IN (laptop; 4,000+ affected)
 - University Health Care (UT) (laptop; 4,800 affected)
 - As well as: NIH, UCLA Medical Center, UMass Amherst, HealthNow New York, UCSF, and Walter Reed (among many others).
- This does not, unfortunately, include any instances of privacy breaches caused by intentional identity theft by internal employees or loss of paper records.

© 2008 Steven J. Fox



Federal Guidelines

Federal government provides many guidelines, via different departments and agencies, regarding data privacy protection. This presentation will focus on:


- HHS settlement with Providence Healthcare
- Red Flag Rules promulgated by, *inter alia*, the Federal Trade Commission

© 2008 Steven J. Fox



Providence Settlement


© 2008 Steven J. Fox



Providence Settlement

In July 2008, the U.S. Department of Health and Human Services (“HHS”) entered into a settlement agreement with a group of affiliated non-profit health care corporations in Washington and Oregon, Providence Health System (“Providence”), thereby resolving HHS’s investigation into Providence’s breaches of privacy of its patients’ electronic protected health information (“ePHI”) in violation of the HIPAA Privacy and Security Rules.


© 2008 Steven J. Fox



Providence Settlement - Background

- In December 2005, ePHI contained on four backup tapes and two optical disks were left unattended in an employee’s personal car and subsequently stolen.
- The employee followed a standard practice at Providence, known to some managers. Additionally, on four separate dates in 2005 and 2006, laptops containing ePHI were left unattended and were subsequently stolen from employees of Providence.
- The ePHI contained on both the tapes and the laptops was not encrypted.

© 2008 Steven J. Fox



Providence Settlement - CAP

As part of the settlement, Providence agreed to pay HHS \$100,000 and, more importantly, adopt and implement a set of policies, guidelines, and practices to ensure the privacy and security of its patients' ePHI ("Corrective Action Plan" or "CAP").

© 2008 Steven J. Fox



Providence CAP

- The CAP provides a valuable guide for all health care providers seeking to achieve full compliance with HIPAA Privacy and Security Rules. CAP directed Providence to:
 - (a) revise its data security policies and procedures in accordance with the CAP;
 - (b) provide training to all of its employees and future employees regarding such policies and procedures; and
 - (c) to monitor and report on the implementation and operation of the new security guidelines.

© 2008 Steven J. Fox



Providence CAP – Minimum Requirements

- The CAP mandated the following minimum requirements for the new ePHI security policies and procedures:
 - Conduct a risk assessment of potential risks and vulnerabilities to confidentiality, integrity and availability of ePHI when it is created, received, maintained, used or transmitted offsite;
 - Implement security measures to minimize the risks identified in the risk assessment;

© 2008 Steven J. Fox



Providence CAP – Minimum Requirements (cont'd)

- Provide physical safeguards governing off-site storage and transport of backup electronic media containing ePHI, as well as governing physical security of portable devices containing ePHI;
- Provide technical safeguards governing encryption of backup electronic media and portable containing ePHI (including password protection and other safeguards); and
- Report any noncompliance to HHS within 30 days of occurrence, including a description of any actions taken by Providence to mitigate any harm and prevent such events from recurring.

© 2008 Steven J. Fox



Providence CAP - Training

- The CAP also required Providence to “provide evidence” to HHS that Providence *trained* its workforce on the new policies and procedures, especially all the personnel with access to the ePHI. Other training requirements include:
 - Training new employees with access to ePHI within 30 days of beginning their service;
 - Each employee receiving the training certifying in writing that she/he received the required training, and indicating the date of the training;

© 2008 Steven J. Fox



Providence CAP – Training (cont'd)

- Retaining and reviewing (at least annually) all training materials, and updating such materials to reflect any changes in applicable law or to correct any issues discovered during audits or reviews; and
- Prohibiting employees who did not receive the required training from access to back up media or portable devices containing ePHI.

© 2008 Steven J. Fox



Providence CAP - Monitoring

- The CAP also imposed a significant requirement on Providence to monitor the protected data environment by
 - Validating that its workforce is familiar and continually complies with the data security policies and procedures;
 - Ensuring that all electronic media and portable devices containing ePHI comply with the same policies;

© 2008 Steven J. Fox



Providence CAP – Monitoring (cont'd)

- As part of monitoring, conducting of quarterly reviews, which encompass unannounced visits to Providence facilities, interviews with samples of Providence workforce with access to media or portable devices containing ePHI, and inspection of random samples of such devices;
- Using such reviews to identify any risks to security of ePHI, develop recommendations to reduce such risks to a reasonable level, and ensure that such recommendations are implemented;
- Finally, documenting such results and making all documentation (including summaries of inspections, assessments or risk, and risk mitigation recommendations) available to HHS.

© 2008 Steven J. Fox



Red Flag Rules (Identity Theft Program)

© 2008 Steven J. Fox



Red Flag Rules

- Federal Trade Commission's Red Flag rules, adopted in November of 2007, are intended to combat widespread identity theft in many sectors of the economy.
- Full compliance with the Red Flag rules was originally set for November 1, 2008.
- But due to widespread confusion as to the applicability of the rules, on October 22, FTC announced it will "suspend enforcement" for six months until May 1, 2009.

© 2008 Steven J. Fox



Red Flag Rules

- Delay will enable entities to develop and implement identity theft prevention programs.
- Note that the delay is limited to the Identity Theft Red Flag Rule (16 CFR 681.2) and does *not* extend to the rule regarding address discrepancies applicable to users of consumer credit reports (16 CFR 681.1)

© 2008 Steven J. Fox



Red Flag Rules

- A Red Flag is defined as a pattern or practice that indicates the possible existence of identity theft.
- Entities subject to this regulation include financial institutions, creditors, credit and debit card issuers and users of consumer credit reports.
 - For example, healthcare providers *may* be covered entities if they are "creditors" under the definition provided in the Fair Credit Reporting Act.

© 2008 Steven J. Fox



Red Flag Rules

Federal law defines a creditor as:

- any entity that regularly extends, renews, or continues credit;
- any entity that regularly arranges for the extension, renewal, or continuation of credit; or
- any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.
- Accepting credit cards as payment does not automatically make an entity a creditor.

© 2008 Steven J. Fox



Red Flag Rules – Identity Theft Prevention Program

- The first and most significant requirement of the Red Flag rules is development and implementation of an Identity Theft Prevention program (“Program”) for each covered entity, and applicable solely for such entity’s **“covered accounts.”**
- Covered accounts include accounts designed to permit multiple payments or transactions
 - (e.g., credit card accounts, accounts for patients, and even business credit accounts may be covered under this regulation.)

© 2008 Steven J. Fox



Red Flag Rules – Identity Theft Prevention Program

- With the full compliance requirement looming in six months, covered entities should take the following steps:
 - Assess whether your organization possesses “covered accounts”;
 - Assess current practices aimed at preventing identity theft. You can utilize the existing privacy or identity theft prevention programs or policies, including policies and processes regarding background checks, system access audits under HIPAA, and other privacy policies;

© 2008 Steven J. Fox



Red Flag Rules – Identity Theft Prevention Program

- Secure buy-in, participation and sponsorship from the senior management and the board of your organization. The Board of your organization must approve the Program; and
- Secure participation of all relevant parties within your organization in developing and implementing the Program, including management, legal, accounting, information technology, compliance and/or audit department representatives.
 - This should also include appropriate personnel to ensure successful training of all relevant staff.

© 2008 Steven J. Fox



Red Flag Rules – Identity Theft Prevention Program

- The Program must be designed to “detect, prevent, and mitigate identity theft” in connection with the covered accounts. The Program must provide for:
 - **Policies and procedures for identifying, detecting and responding to Red Flags**
 - e.g., notifications from credit reporting agencies, alerts initiated by customers or patients, inappropriate or suspicious use of customer’s accounts.
 - **Flexibility** because the Program needs to be an evolving document, enabling modifications or updates to the Program based on newly identified risks or other Red Flags;

© 2008 Steven J. Fox



Red Flag Rules – Identity Theft Prevention Program

- Cont’d. The Program must provide for:
 - **Board level approval and senior management oversight.**
 - The Board must not only approve the Program’s implementation, but also be informed of the Program’s effectiveness annual reports to the Board. Such annual reports should assess the program’s effectiveness, cite all significant incidents involving identity theft and management’s responses thereto, and recommend any changes to the Program based on such assessment;

© 2008 Steven J. Fox



Red Flag Rules – Identity Theft Prevention Program

- Other requirements include:
 - **Training of staff to manage the Program.**
 - Red Flag rules mandate an effective implementation of the Program. Training is crucial to such effective implementation (including training varied by department or individual role in the Program). Training should also be ongoing to ensure staff's knowledge of the latest Red Flags and other newly discovered risks; and
 - **Oversight of service provider arrangements (e.g., outsourcers, data or payment processors, and business associates).**
 - Service provider arrangements should also be included in management's annual report to the Board.

© 2008 Steven J. Fox



Red Flag Rules – Identity Theft Prevention Program

- Cont'd. Other requirements include:
 - **FTC requires that each Program must be formulated with consideration of detailed Guidelines that add substance to the above requirements.**
 - Such Guidelines, along with a sample list of Red Flags, may be found in the Federal Register, Vol. 72, No. 217, Friday November 7, 2007 (Appendix A to Part 681 - 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation).

© 2008 Steven J. Fox



What should you do?

- The Providence CAP and the Red Flag Rules provide valuable guidance for all health care providers as they continually reevaluate their own policies, procedures and training schedules.
- We encourage health care providers to
 - carefully consider the guidelines for each of these requirements, outlined above, and
 - take the necessary steps to create and implement the right set of policies and procedures that would safeguard your organization from privacy or security breaches.

© 2008 Steven J. Fox



QUESTIONS?

© 2008 Steven J. Fox



Q&A

For additional information, please feel free to contact:

- Steven J. Fox at SJFox@PostSchell.com (202-661-6940) or
- Vadim Schick at VSchick@PostSchell.com (202-661-6945)
- www.PostSchell.com

© 2008 Steven J. Fox

