September 2012 Vol. 12, No. 9

BRIEFINGS ON HIPAA

• Privacy • Security • Transactions • Training

HIPAA audits

OCR protocol information a valuable compliance tool

It may not be the proverbial keys to the kingdom, but OCR's recently published audit protocol for its current privacy and security audits gives healthcare organizations an inside look at the inspection process.

OCR's publication of the audit protocol on its website in June identified the numerous procedures that KPMG—the auditor hired by OCR to conduct 115 audits in 2012—is using to measure compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

The protocol offers a glimpse behind the audit curtain, giving organizations a tool to prepare for potential audits and help ensure HIPAA compliance. The audit protocol organization relies on modules that represent elements of privacy, security, and breach notification.

Key activities

The protocol includes 165 key activities—78 related to the Privacy Rule, 77 related to the Security Rule, and 10 related to breach notification.

Want to know how to perform well if your organization is selected for one of the random HIPAA audits? The protocol suggests that robust documentation of your compliance efforts is key, says **Adam H. Greene, JD, MPH,** a partner at Davis Wright Tremaine, LLP, in Washington, D.C., and until recently an OCR regulator. However, the protocol leaves many unanswered questions about the requirements upon which covered entities are being assessed, Greene says.

This month's tip—
Learn how to tailor an education and training program to your organization's specific compliance needs on p. 6.

For example, the protocol doesn't really answer some of the nagging questions about how frequently organizations must perform some of the tasks required by the regulations or how much detail is necessary, he says.

"But it's more helpful than not," says Greene, who considers it additional information that can help organizations comply with HIPAA.

Organizations expecting a quick ticket to HIPAA compliance won't find it in the protocol, says **Phyllis A. Patrick, MBA, FACHE, CHC,** founder of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y.

"There's nothing really new here. If organizations are familiar with the standards and are following them, they have little to worry about," she says.

The protocol lists key activities—tasks such as conducting a risk assessment, notifying affected individuals of a breach, and ensuring minimum necessary uses of PHI. It lists established performance criteria rather than actual standards, but the language derives directly from HIPAA rules. Audit procedures for each performance criteria explain how auditors will ask the organizations

IN THIS ISSUE

to demonstrate compliance. A specific activity could have numerous audit procedures that measure compliance.

Organizations can transform the protocol into a useful checklist by adding a column for findings to describe compliance efforts, Patrick says. For example, an organization might note that it has adopted but not yet implemented a policy. Add another column for recommendations—tasks an organization must perform to satisfy the standards and demonstrate compliance to an audit team.

"I think it is valuable, especially for people who haven't put together a tool," says Patrick. "This is a good way to look at it. It reaffirms what is in the standards. The content is still the same."

Briefings on HIPAA (ISSN: 1537-0216 [print]; 1937-7444 [online]) is published monthly by HCPro, Inc., 75 Sylvan St., Suite A-101, Danvers, MA 01923. Subscription rate: $349/year. • **Briefings on HIPAA,** P.O. Box 3049, Peabody, MA 01961-3049. • Copyright © 2012 HCPro, Inc. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro, Inc., or the Copyright Clearance Center at 978-750-8400. Please notify us immediately if you have received an unauthorized copy. • For editorial comments or questions, call 781-639-1872 or fax 781-639-7857. For renewal or subscription information, call customer service at 800-650-6787, fax 800-639-8511, or email *customerservice@hcpro.com.* • Visit our website at *www.hcpro.com.* • Occasionally, we make our subscriber list available to selected companies/vendors. If you do not wish to be included on this mailing list, please write to the marketing department at the address above. • Opinions expressed are not necessarily those of **BOH.** Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions.

For example, an organization can review its breach notification reporting policy. Organization leadership can use the protocol to determine whether its policy includes all of the necessary components.

HIPAA privacy and security officers can use it to educate staff about the HIPAA requirements, says Patrick. The protocol summarizes the activities that organizations should undertake. Greene and Patrick agree that the audit protocol is another valuable tool for organizations.

Pros and cons

OCR's audit protocol has positive and negative aspects, says Greene. On the positive side, it provides questions that the audit teams will ask to measure HIPAA compliance.

For example, a series of questions follows the Security Rule key activity pertaining to terminating workforce members' access to information systems when it's no longer necessary or appropriate. Audit teams ask management how user access is eliminated upon termination or change of position on a timely basis. They also request and review policies and procedures to determine how an organization terminates user access.

Organizations can review the questions themselves and conduct a gap analysis, says Greene says, adding that the result should be an improved privacy and security program.

The protocol and other free tools are being provided by the government and should help organizations move forward in the direction of HIPAA compliance, Greene says. The audit protocol, along with the recently published *National Institute of Standards and Technology (NIST) HIPAA Security Rule Toolkit* and training videos provided to state attorneys general, offer a wealth of valuable information, he says.

However, the protocol is not comprehensive and it lacks specificity, Greene notes. For example, the contract with KPMG indicates that the audit protocol will include interview questions written to accommodate organizations of varying type and size. "None of that comes through here," he says.

Organizations nonetheless can make good use of the protocol. "I think they can use this as a good baseline. Organizations can go through the protocol questions and answer 'yes' or 'no,' " Greene says.

They can check to see whether they have documentation the audit teams will request and ensure they can respond to each element of the protocol questions. "The caution is that that shouldn't be the end. Stop, sit down, and think. Look at what's working and what's not," he says.

Patrick believes OCR should let covered entities and business associates decide what is right for their organizations and not dictate too many specifics.

"The Security Rule in particular was meant to be flexible and scalable to fit organizations of different types and sizes," she says. "By being proactive and defining your security and privacy programs in terms and ways that suit your organization, you can take comfort that you are doing the right thing."

"Don't make it too complex. Security and privacy are pretty basic concepts and healthcare professionals are trained to protect privacy and put the patient first," she says.

Three important questions

Three questions capture the essence of the HIPAA compliance audits, says **Bob Chaput, CISSP, CIPP/US, CHP, CHSS,** CEO and founder of Clearwater Compliance, LLC, a HIPAA-HITECH consultant in Nashville.

1. **Is it documented?** You must have policies, procedures, and documentation, he says. The auditors will expect to see the manuals, logs, and evidence that you are following HIPAA regulations.
2. **Are you doing it?** Establishing policies and procedures isn't enough; you must also implement them. You must use, apply, practice, and enforce policies and procedures, Chaput says. If an audit team reviews your policy that requires encryption of all laptop computers, but sample testing reveals a dozen are unencrypted, this is a problem.
3. **Is it reasonable and appropriate?** This language appears throughout the Privacy and Security Rules, says Chaput, adding that OCR does not expect one size to fit all. What's reasonable and appropriate for a major teaching hospital might not be for a solo physician practice. The threats, risks, and vulnerabilities may be very different. ■

Editor's note: Access the OCR audit protocol at http://ocrnotifications.hhs.gov/hipaa.html. *Patrick has posted the protocol in spreadsheet format, available on her website at* www.phyllispatrick.com.

To download the NIST HIPAA Security Rule Toolkit, *visit* http://scap.nist.gov/hipaa.

You can access training videos provided to state attorneys general at www.hhshipaasagtraining.com.

OCR HIPAA audit protocol key activities

The audit protocol includes 165 activities related to the HIPAA Privacy, Security, and Breach Notification Rules. Duplicates reflect applicablity to more than one audit procedure.

Security Rule

The 77 key activities related to the Security Rule include the following:

1. Conduct risk assessment
2. Acquire IT systems and services
3. Develop and deploy the information system activity review process
4. Development and implement a sanction policy
5. Select a security official to be assigned responsibility for HIPAA security
6. Assign and document the individual's responsibility
7. Establish clear job description and responsibilities
8. Establish criteria and procedures for hiring and assigning tasks
9. Establish workforce clearance procedures
10. Establish termination procedures
11. Implement policies and procedures for authorizing access
12. Implement policies and procedures for access establishment and modification
13. Isolate healthcare clearinghouse functions
14. Evaluate existing security measures related to access controls
15. Develop and approve a training strategy and plan
16. Develop and approve a training strategy and plan
17. Protection from malicious software; login monitoring; and password management
18. Develop appropriate awareness and training content, materials, and methods
19. Implement the training
20. Implement security reminders
21. Monitor and evaluate the training plan
22. Develop and implement procedures to respond to and report security incidents
23. Develop and implement procedures to respond to and report security incidents
24. Develop a contingency planning policy
25. Data backup plan and disaster recovery plan
26. Develop and implement an emergency mode operation plan
27. Testing and revision procedure
28. Identify preventive measures
29. Develop recovery strategy
30. Data backup plan and disaster recovery plan
31. Determine whether internal or external evaluation is most appropriate
32. Develop standards and measurements for reviewing all standards and implementation specifications of the Security Rule
33. Conduct evaluation
34. Document results
35. Repeat evaluations periodically
36. Written contract or other arrangement
37. Implement an arrangement other than a business associate contract if reasonable and appropriate
38. Conduct an analysis of existing physical security vulnerabilities
39. Develop a facility security plan
40. Establish contingency operations procedures
41. Establish contingency operations procedures
42. Maintain maintenance records
43. Identify workstation types and functions or uses
44. Identify expected performance of cache type of workstation
45. Analyze physical surroundings for physical attributes
46. Identify all methods of physical access to workstations
47. Identify and implement physical safeguards for workstations
48. Implement methods for final disposal of ePHI
49. Maintain accountability for hardware and electronic media
50. Develop data backup and storage procedures
51. Develop data backup and storage procedures
52. Develop and implement procedures for reuse of electronic media
53. Encryption and decryption
54. Analyze workloads and operations to identify the access needs of all users
55. Identify technical access control capabilities

56. Ensure that all system users have been assigned a unique identifier
57. Develop access control policy
58. Implement access control procedures using selected hardware and software
59. Implement access control procedures using selected hardware and software
60. Implement access control procedures using selected hardware and software
61. Review and update user access
62. Establish an emergency access procedure
63. Establish an emergency access procedure
64. Automatic logoff
65. Terminate access if it is no longer required
66. Determine the activities that will be tracked or audited
67. Select the tools that will be deployed for auditing and system activity reviews
68. Develop and deploy the information system activity review/audit policy
69. Develop appropriate standard operating procedures
70. Identify all users who have been authorized to access ePHI
71. Implement procedures to address these requirements
72. Implement a mechanism to authenticate ePHI
73. Determine authentication applicability to current systems/applications
74. Evaluate authentication methods available
75. Select and implement authentication option
76. Select and implement authentication option
77. Develop and implement transmission security policy and procedures

Breach Notification Rule

The 10 key activities related to the Breach Notification Rule include the following:

1. Risk assessment of breach
2. Notification to individuals
3. Timeliness of notification
4. Methods of individual notification
5. Content of notification
6. Notification to the media
7. Notification to the secretary
8. Notification by a business associate
9. Law enforcement delay
10. Burden of proof

Privacy Rule

The 78 key activities related to the HIPAA Privacy Rule are as follows:

1. Deceased individuals
2. Personal representatives
3. Uses and disclosures consistent with notice
4. Disclosures by whistleblowers
5. Disclosures by workforce members who are victims of a crime
6. Confidential communications
7. Requirements for group health plans
8. Requirements for a covered entity with multiple covered functions
9. Permitted uses and disclosures
10. Consent for uses and disclosures
11. Authorizations for uses and disclosures is required
12. Compound authorizations
13. Prohibition on conditioning of authorizations
14. Limited uses and disclosures when the individual is not present
15. Use and disclosure for facility directories
16. Uses and disclosures for facility directories in emergency circumstances
17. Permitted uses and disclosures
18. Uses and disclosures with the individual present
19. Uses and disclosures for disaster relief purposes
20. Opportunity to object
21. Uses and disclosures for research purposes
22. Uses and disclosures for research purposes
23. Uses and disclosures required by law
24. Uses and disclosures for public health activities
25. Disclosures about victims of abuse, neglect, or domestic violence
26. Uses and disclosures for health oversight activities
27. Disclosures for law enforcement purposes
28. Disclosures for law enforcement purposes
29. Disclosures for law enforcement purposes

OCR HIPAA audit protocol key activities *(cont.)*

30. Disclosures for law enforcement purposes
31. Disclosures for law enforcement purposes
32. Uses and disclosures about decedents
33. Uses and disclosures for cadaveric organ, eye, or tissue donation
34. Uses and disclosures for specialized government functions
35. Uses and disclosures for specialized government functions
36. Uses and disclosures for specialized government functions
37. Uses and disclosures for specialized government functions
38. Uses and disclosures for specialized government functions
39. Disclosures for workers' compensation
40. Minimum necessary uses of PHI
41. Minimum necessary disclosures of PHI
42. Uses and disclosures for fundraising
43. Uses and disclosures for underwriting and related purposes
44. Verification requirements
45. Limited data sets and data use agreements
46. Limited data sets and data use agreements
47. Re-identification of PHI
48. De-identification of PHI
49. Notice of privacy practices
50. Provisions of notice—health plans
51. Provisions of notice—certain covered healthcare providers
52. Provisions of notice—electronic notice
53. Joint notice by separate covered entities
54. Documentation
55. Confidential communications requirements
56. Terminating a restriction
57. Documentation
58. Right of an individual to request restriction of uses and disclosures
59. Right to access
60. Review of denial of access
61. Unreviewable ground for denial
62. Reviewable grounds for denial
63. Documentation
64. Right to amend
65. Denying the amendment
66. Accepting the amendment
67. Denying the amendment
68. Right to an accounting of disclosures of PHI
69. Content of the accounting
70. Provision of the accounting
71. Documentation
72. Training
73. Complaints to the covered entity
74. Sanctions
75. Policies and procedures
76. Administrative, technical, and physical safeguards
77. Mitigation
78. Refraining from intimidating or retaliatory acts

Editor's note: Access the OCR audit protocol at *http://ocrnotifications.hhs.gov/hipaa.html.*

Compliance building blocks

Education and training are essential components

Education is giving people the knowledge they need. Training helps them develop the skills that allow them to put that knowledge to use.

Both are important with respect to your workforce and the knowledge necessary to comply with HIPAA and other rules and regulations, says **Frank Ruelas, MBA,** principal of HIPAA College, based in Casa Grande, Ariz.

You must educate and train your entire workforce, which includes employees, vendors, and volunteers. Don't just consider the education and training your staff members need, says Ruelas. HIPAA compliance requires that you train all of your employees, as well as vendors and volunteers who come into contact with any of your patients' PHI.

Content

Education is all about attaining knowledge. Ensure that your compliance program includes educating your workforce about applicable regulations. Address all regulations that apply to your organization, including

HIPAA and others such as the Emergency Medical Treatment and Active Labor Act (EMTALA).

Your workforce must be aware of your compliance program policies and procedures. Consider your risk areas and raise workforce awareness about them, Ruelas says. For example, if you are experiencing issues that pertain to billing, this should drive the content of your education.

Make your education applicable to what is happening in your own organization and what your workforce members need to know. If your organization has experienced the loss or theft of laptop computers, focus education efforts on your policies that help protect PHI on those computers. If workforce members take files that might contain PHI off-site, educate them about your policy governing removal of PHI from your premises.

Review and revise your content. This is where some organizations fail, Ruelas says. Issues may change, and your content must reflect this.

Requirements

You will also face requirements for your training and education based on the various regulations you must follow. Who must attend training? What kind of records must you retain? Documenting the education and training you provide to workforce members is essential. Who attended the training and when was it completed? How long must you retain these records? HIPAA requires that your organization retain the records for six years.

Also, consider the schedule for providing education and training. Initial training and education is necessary for all new workforce members during orientation. Provide continuing education that reviews and updates this information.

Flexibility is necessary so that you can offer additional training when issues or problems arise, says Ruelas. Consider how soon you can begin training your workforce after identifying a problem.

This training can help prevent problems from occurring in the future. For example, improper disposal of records containing PHI by your staff is a problem that requires your attention before a breach occurs. Likewise, staff members who leave file cabinets containing patient records unlocked or share computer passwords require reeducation about your security policies and procedures.

Consider the different levels of training necessary. Workforce members in different departments will likely require different levels of training. For example, EMTALA requires hospitals to provide care to anyone who needs emergency healthcare. However, the education provided to healthcare workers in your emergency department will differ significantly from the training you provide your food services staff.

All workforce members must have a basic understanding with respect to how HIPAA protects patient privacy and security. However, what physicians and nurses need to know differs from what members of your safety department need to know, so customize your education and training accordingly.

Training

The content of education and training helps establish your mode of delivery. Some content lends itself to computer-based learning; other content may be more suitable for a classroom setting or departmental meetings.

Finally, ensure that workforce members sign a statement attesting that they have completed training. ■

Editor's note: This is the third in a series on basic compliance featuring expert Frank Ruelas, MBA. In this series, Ruelas introduces those new to compliance to some basic principles proven helpful in establishing effective compliance programs.

Questions? Comments? Ideas?

Contact Contributing Editor
Joanne Finnegan
Email *joannef100@hotmail.com*

Expert advice about mobile devices

Don't let inadequate security be your downfall

Mobile devices—thumb drives, smartphones, external hard drives, tablets, and laptop computers—are creating risks for PHI exposure.

These mobile devices are increasingly exposing PHI, with the risk of privacy incidents increasing, according to the U.S. Department of Homeland Security (DHS).

Security threats against mobile devices include introduction of spyware and other malicious software, loss of treatment records or test results, and theft of patient data, according to the DHS report "Attack Surface: Healthcare and Public Health Sector." It states: "Since wireless medical devices are now connected to medical networks, information technology networks are now remotely accessible through the medical device."

The rapid adoption of electronic health records is also accelerating the use of mobile devices in healthcare.

Because staff can move, process, and share patient data on personal cell phones and tiny USB flash drives, the "bring your own device" (BYOD) phenomenon is posing new challenges for healthcare organizations.

How can you help reduce privacy incidents that are the result of mobile risks?

Experts who work in legal, data breach prevention, technology, healthcare IT, and security offer 13 recommendations for consideration by your healthcare organization.

USB locks

Install USB locks on desktop computers, laptop computers, and other devices that may contain PHI or sensitive information. This step can prevent unauthorized data transfer—both uploads or downloads—through USB ports and thumb drives, says **Christina Thielst, FACHE,** vice president at the Tower Consulting Group, based in Playa Vista, Calif.

The device easily plugs ports as a low-cost solution and offers an additional layer of security when you install encryption or other software, Thielst says.

Geolocation tracking software

Consider geolocation tracking software or services for mobile devices, says **Rick Kam, CIPP,** president and cofounder of ID Experts in Portland, Ore. Geolocation tracking software is a low-cost insurance policy against loss or theft that can immediately track, locate, or wipe the device of all data, says Kam.

Most healthcare organizations currently lack sufficient resources to prevent or detect unauthorized patient data access, loss, or theft. Lost or stolen computing or data devices are the top reason for healthcare data breach incidents, Kam says.

'Brick' lost and stolen mobile devices

"Brick" the mobile device when it is lost or stolen, says **Jon A. Neiditz, Esq.,** a partner at Nelson Mullins Riley & Scarborough, LLP's Atlanta office.

Employee acceptance of "remote wipe" processes that "brick" an entire device when it is lost or stolen instead of simply deleting the encrypted silo of corporate information has grown in the past year, Neiditz says.

Bricking an entire device is more acceptable because personal data is now more frequently backed up in cloud storage, so bricking an entire device does not result in data loss, and it protects employees and employers, he says.

Neiditz recommends healthcare organizations implement this as a first step in protecting against breaches from BYOD devices.

Encryption

Encrypt, advises **Chris Apgar, CISSP,** president and CEO of Apgar and Associates, LLC, in Portland, Ore.

You should encrypt all mobile devices and the often-overlooked media, such as USB drives, if workforce members will use them remotely, says Apgar. The cost of encryption is modest and it is sound insurance against what has been demonstrated to be a significant risk to healthcare organizations.

Most breaches do not occur because of cybercrime, Apgar says. Rather, they are associated with people. Even if organizations allow employees to use their own tablets, laptop computers, and smartphones, they should require encryption if the possibility that sensitive data will be stored on these devices exists, Apgar says.

Organizations might have policies that prohibit the storage of sensitive information on personally owned devices, but they are very difficult to enforce, he cautions. At the very least, organizations should require use of company-owned and encrypted portable media.

Shut down laptop computers

Shut down laptop computers completely instead of using sleep mode, which can render encryption products ineffective, says **Winston Krone,** managing director at Kivu Consulting in San Francisco.

Healthcare organizations now routinely install full-disk encryption on employees' laptop computers, he says.

However, most of the leading encryption products are configured so that entering a password disables encryption, leaving a laptop computer unprotected, until the laptop computer is booted down, meaning it is shut down and restarted. Simply putting a laptop computer in sleep mode does not reactivate encryption protection. A laptop computer that is lost or stolen while in sleep mode is completely unprotected.

Organizations should clearly advise workforce members to completely shut down laptop computers before removing them from the workplace and to always use the full shutdown function rather than sleep mode when traveling or leaving a laptop unattended in an unsecure environment.

Organizations should strictly enforce and audit this policy, Krone says.

Personal mobile devices

Recognize that workforce members may use personal mobile devices to handle PHI, even if it is contrary to your policy, says **Adam Greene, JD, MPH,** a partner at Davis Wright Tremaine, LLP, in Washington, D.C.

Healthcare organizations should consider documenting this in their risk assessments and identify safeguards established to limit inappropriate use of personal devices (e.g., strong policies, training, sanctions for noncompliance), Greene says.

Further reduce the risk by considering the root cause of the problem—what benefits do personal devices offer employees that an organization's systems lack? For example, if clinicians text PHI from personal devices because a hospital does not offer a similarly convenient means of communication, consider offering a secure alternative to texting, Greene says.

Strong technical safeguards

Don't permit access to PHI via mobile devices without strong technical safeguards, says **Kelly Hagan, Esq.,** of Schwabe, Williamson & Wyatt in Portland, Ore. These safeguards include encryption, data segmentation, remote data erasure and access controls, and virtual private network software.

Mobile devices are an OCR enforcement priority and justify significant investment in secure technology by covered entities, Hagan says. If such technology is beyond an organization's means, then it should not permit mobile device access, he says. Mobile devices are inherently insecure and may end up costing the organization much more than supplying good technical safeguards, he says.

Education

Educate employees about the importance of safeguarding their mobile devices, says **Larry Ponemon, PhD, CIPP,** chairman and founder of the Ponemon Institute in Traverse City, Mich.

Risky behavior includes downloading applications and free software from unsanctioned online stores that may contain malware, turning off security settings, failing to encrypt data in transit or at rest, and failing to promptly report lost or stolen devices that may contain confidential and sensitive information.

Security of ePHI

Implement ePHI security, says **Christine Marciano,** president of Cyber Data Risk Managers, LLC, a data breach insurance company in Freehold, N.J.

Marciano considers ePHI the biggest issue healthcare organizations face when using mobile devices and creating a BYOD policy. Accessing ePHI from a multitude of mobile devices significantly increases the risks of system contamination by viruses introduced by mobile devices, she says.

Mobile devices and BYOD policies leave a healthcare organization open to potential data breaches.

Healthcare organizations should consider purchasing cyber liability insurance as part of their data breach response plans to protect themselves and the PHI they manage against these increased vulnerabilities, Marciano says.

Device disposal and donation

Ensure that devices coming offline are adequately secured and checked before disposal or donation, says **Richard Santalesa, Esq.,** senior counsel at the Information Law Group in Fairfield, Conn.

Doing so helps ensure that a healthcare organization gets ahead of the BYOD upgrade curve, he says.

Recognize human nature for what it is, and anticipate that staff will sidestep even firm and clear information security policies, Santalesa says. One concern with BYOD is that users own and are primarily in control of their devices—not your IT department.

Devices coming offline when users upgrade to new smartphones or mobile devices are almost always overlooked, he says.

Smartphones and other devices typically become toys for children, are donated to various charitable organizations, or given to other family members, often without confirmation that they've been sufficiently wiped clean. This leaves potentially sensitive, confidential, and other data intact, Santalesa says. The result is a constant stream of devices going offline and posing significant data breach risks.

Proactive data management strategy

Implement a proactive data management strategy, says **Chad Boeckman,** president of Secure Digital Solutions, LLC, in Saint Louis Park, Minn.

As an increasing number of healthcare practitioners use mobile devices to access patient information, proactive data management strategy has never been more important, he says.

The healthcare industry can adopt data protection concepts from the financial industry, Boeckman says. For example, credit cards increasingly are sent with tokenization technology. This technology can be adopted for the healthcare industry to allow access to patient data on an as-needed basis. The goal of this strategy is protecting critical patient data through access profiles specifically for mobile devices and related applications.

Accessing sensitive information with mobile devices will increase, particularly with greater adoption of electronic medical record systems and complimentary mobile applications that allow easy access outside the office, Boeckman says.

Transparency and end-user opt-in

Require transparency and end-user consent opt-in, says **David Allen,** chief technology officer at Locaid Technologies in San Francisco. Clear and explicit user opt-in is essential for maintaining a positive brand perception and authenticity for any company collecting, sharing, and/or storing personal information, he says.

Google, Apple, and other popular smartphone applications were publicly scorned earlier this year for compiling user information, including location data, and actual names, email addresses, and telephone numbers in users' address books.

Data collection is not the problem; litigation focuses on the lack of transparency and consumer consent.

Not your father's Internet

Finally, always remember that the mobile Web and "app" landscape is not your father's Internet, says **Pam Dixon,** executive director of World Privacy Forum in San Diego, a nonprofit public interest research group that focuses on privacy research, analysis, and consumer education.

Conducting a thorough technical review and risk audit of these new technologies before implementation is important, she says. Assessments must include how and when patients and/or employees will use the technology.

Many healthcare providers are considering developing or using apps, especially for tablets and iPhone® devices. "I've seen everything from single apps like iPhone glucometers to providers handing out tablets for full 'clinic in hand' programs," Dixon says.

A healthcare provider that is developing its own app or mobile clinic tablet must ensure that its development team consults legal, privacy, and compliance counsel to anticipate and prevent future problems. "Compliance always needs to win, and developers need to really understand that," Dixon says. ■

Editor's note: Access the DHS report at http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.

Use the following sample form, Integrity of PHI at ABC Organization, as the basis for demonstrating compliance when organization-specific details are added. This form is from The No-Hassle Guide to HIPAA Policies: A Privacy and Security Toolkit *published by HCPro, Inc.*

Integrity of PHI at ABC Organization

The HIPAA Security Rule calls for data integrity measures under the Technical Safeguards section of the rule. These are:

1. A required integrity standard [164.312(a)(1)] with an underlying, addressable implementation specification calling for mechanisms to ensure the integrity of an organization's electronic PHI (presumably at rest).
2. An addressable implementation specification under the Transmission Security standard [164.312(e)(1)] calling for mechanisms to ensure integrity of ePHI in transit.

Since integrity is one of the three major principles of information security, along with confidentiality and availability, it is obvious that a covered entity's information security program must take steps to ensure the integrity of protected information.

This organization complies with HIPAA's integrity requirements through a variety of mechanisms.

Administrative mechanisms

All users with access to ePHI are required to be formally authorized for such access, and only when required for performance of one's job. (See policy XXX, procedure YYY, and form ZZZ.)

Access is granted at the minimum necessary level for job performance. For example, front desk users who do not need access to clinical data do not receive clinical data access (within the technical capabilities of the system). And users needing inquiry access only do not receive update capability. (See policy XXX.)

All users with access to ePHI are issued unique user IDs so that activity can be traced back to an individual. (See policy XXX.)

User access to ePHI requires user authentication, such as passwords, meeting organization standards. (See policy XXX and Password Standards.)

Processes are in place (a) to periodically review who has access to ePHI and (b) to frequently review logs of system activity.

Integrity of PHI at ABC organization *(cont.)*

(See policy XXX and Information System Activity Review Procedures.)

The workforce receives training on use of the ePHI application(s), including performing data entry/update, and security training on (see Training Modules XXX):

- Password management
- Protecting the workstation and materials
- Reporting security incidents
- Users who no longer need access (e.g., terminations) cannot access protected systems
- Data backup and recovery procedures are thoroughly documented to minimize the impact of a system failure

The mechanisms above help ensure that only users with a work-related need are granted access to ePHI, and that user access is limited to the data and functions needed (within the technical limitations of the system). Training helps ensure that users with ePHI access know how to use the system(s) correctly so that they do not inadvertently corrupt data, and so that they behave in ways that prevent unauthorized access. Contingency plans including backup and recovery processes preserve data integrity in case of a system disaster.

Physical mechanisms

This organization's facility security plan (see XXX) and data center protections such as entry locks, backup power supply, temperature controls, and fire-suppression tools, help preserve ePHI integrity.

Technical mechanisms

This organization's systems containing or using ePHI employ the following features that help ensure data integrity:

- Application-level edits on data entry fields
- Entry fields using drop-down menus of codes instead of using free-format data entry
- Double-keying of critical data entry fields such as manual lab results [Be sure to include only if applicable]
- Record counters (input records, output records, error and exception records) and reporting
- Audit trails recording access to, and activity within, the system
- Method of recording all data adds/updates/deletes for disaster recovery

Additionally, this organization uses:

- Antimalware software to prevent data corruption or destruction
- Selective encryption to prevent unauthorized access (and, hence, lessen the possibility of data corruption) [Be sure to include only if applicable—refer to documentation of what/where/how encryption is used]
- Selective file-integrity checking [Be sure to include only if applicable—refer to documentation of what product, such as Tripwire, and what files are checked, etc.]
- Standard error-correcting memory and disk storage
- Database integrity checking [Be sure to include only if applicable—refer to documentation of where/what/how]
- Standard network protocols containing integrity and error-checking mechanisms such as CRC
- Message hashing [Be sure to include only if applicable—refer to documentation of where/what/how]

A supplement to **Briefings on HIPAA**

Privacy & Security Primer

A training tool for healthcare staff

September 2012

Tips from this month's issue

OCR HIPAA audit protocol (p. 1)

1. OCR's publication of the audit protocol on its website in June identified the numerous procedures being used to measure compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

2. Organizations can use the audit protocol to prepare for potential audits and help ensure HIPAA compliance.

3. Audit protocol modules represent elements of privacy, security, and breach notification.

4. Access the OCR HIPAA audit protocol at *http://ocrnotifications.hhs.gov/hipaa.html.*

5. Three questions capture the essence of the HIPAA compliance audits:

- **Is it documented?** You must have policies, procedures, and documentation. Auditors will expect to see the manuals, logs, and evidence that you are following HIPAA regulations.
- **Are you doing it?** Establishing policies and procedures isn't enough; you must also implement them. If an audit team reviews your policy that requires encryption of all laptop computers, but sample testing reveals a dozen are unencrypted, this is a problem.
- **Is it reasonable and appropriate?** This language appears throughout the Privacy and Security Rules. OCR does not expect one size to fit all. What's reasonable and appropriate for a major teaching hospital might not be for a solo physician practice. The threats, risks, and vulnerabilities may be very different for such different entities.

Compliance building blocks (p. 6)

6. Education is giving people the knowledge they need. Training helps them develop the skills that allow them to put that knowledge to use.

7. You must educate and train your entire workforce, which includes employees, vendors, and volunteers. Don't just consider the education and training your staff members need. HIPAA compliance requires that you train all of your employees, as well as vendors and volunteers who come into contact with any of your patients' PHI.

8. Education is about attaining knowledge. Ensure that your compliance program includes educating your workforce about applicable regulations, such as HIPAA and the Emergency Medical Treatment and Active Labor Act.

9. Your workforce must be aware of your compliance program policies and procedures. Consider your risk areas and raise workforce awareness about them. For example, if you are experiencing issues that pertain to billing, this should drive the content of your education.

10. Make your education applicable to what is happening in your own organization and what your workforce members need to know. If workforce members take files that might contain PHI off-site, educate them about your policy governing removal of PHI from your premises.

11. Review and revise your content. This is where some organizations fail. Issues may change, and your content must reflect this.

Mobile device security (p. 8)

12. Security threats against mobile devices include introduction of spyware and other malicious software, loss of treatment records or test results, and theft of patient data, according to a report issued by the U.S. Department of Homeland Security.

13. The rapid adoption of electronic health records is also accelerating the use of mobile devices in healthcare. Because staff can move, process, and share patient data on personal cell phones and tiny USB flash drives, the "bring your own device" (BYOD) phenomenon is posing new challenges for healthcare organizations.

14. Install USB locks on desktop computers, laptop computers, and other devices that may contain PHI or sensitive information. This step can prevent unauthorized data transfer—both uploads or downloads—through USB ports and thumb drives.

15. Consider geolocation tracking software or services for mobile devices. This is a low-cost insurance policy against loss or theft that can immediately track, locate, or wipe the device of all data.

16. "Brick" a mobile device when it is lost or stolen. Employee acceptance of "remote wipe" processes that "brick" an entire device when it is lost or stolen instead of simply deleting the encrypted silo of corporate information has grown in the past year.

17. Encrypt all mobile devices and the often-overlooked media, such as USB drives, if workforce members use them remotely. The cost of encryption is modest and it is sound insurance against what has been demonstrated to be a significant risk to healthcare organizations.

18. Shut down laptop computers completely instead of using sleep mode, which can render encryption products ineffective.

19. Recognize that workforce members may use personal mobile devices to handle PHI, even if contrary to your policy. Consider documenting this in risk assessments and identify safeguards established to limit inappropriate use (e.g., policies, training, sanctions for noncompliance).

20. Don't permit access to PHI via mobile devices without strong technical safeguards.

21. Educate employees about the importance of safeguarding their mobile devices.

22. Implement ePHI security. Accessing ePHI from a multitude of mobile devices significantly increases the risks of system contamination by viruses introduced by mobile devices.

23. Mobile devices and BYOD policies leave a healthcare organization open to potential data breaches. Healthcare organizations should consider purchasing cyber liability insurance as part of their data breach response plans to protect themselves and the PHI they manage against these increased vulnerabilities.

24. Ensure that devices coming offline are adequately secured and checked before disposal or donation.

25. Implement a proactive data management strategy.

26. Require transparency and end-user consent opt-in. Clear and explicit user opt-in is essential for maintaining a positive brand perception and authenticity for any company collecting, sharing, and/or storing personal information.

27. Finally, always remember that the mobile Web and "app" landscape is not your father's Internet.

Privacy and Security Primer is a monthly, two-page **Briefings on HIPAA** insert that provides background information that privacy and security officials can use to train their staff. Each month, we discuss the privacy and security regulations and cover one topic. *September 2012.*