SECOND EDITION

THE NO-HASSLE GUIDE TO EHR POLICIES

Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

HCPro

The No-Hassle Guide to EHR Policies, Second Edition, is published by HCPro, Inc.

First edition published 2006.

ISBN: 978-1-60146-771-3

HCPro, Inc., provides information resources for the healthcare industry.

HCPro, Inc., is not affiliated in any way with The Joint Commission, which owns the JCAHO and Joint Commission trademarks.

Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS, Author
Ilene MacDonald, CPC, Executive Editor
Lauren McLeod, Group Publisher
Janet Morris, Senior Managing Editor
Janell Lukac, Graphic Artist
Adam Carroll, Copyeditor
Amanda Donaldson, Proofreader
Matt Sharpe, Production Supervisor
Susan Darbyshire, Art Director
Jean St. Pierre, Senior Director of Operations

Advice given is general. Readers should consult professional counsel for specific legal, ethical, or clinical questions.

Arrangements can be made for quantity discounts. For more information, contact:

HCPro, Inc.
P.O. Box 1168
Marblehead, MA 01945
Telephone: 800/650-6787 or 781/639-1872
Fax: 781/639-2982
E-mail: *customerservice@hcpro.com*

Visit HCPro online at:
www.hcpro.com and *www.hcmarketplace.com*

11/2010
21828

Contents

Sample Policies

About the Policy Templates

You can download and use the policy templates included within this book as a framework for developing your own policies. These templates offer options to consider. Please note that these templates do not provide recommendations for action.

Although you can modify these templates in any way, consider the following options when you modify them:

- Italicized information in brackets (<*Generic Description*>) describes generic content that you can replace or modify with your organization's specific definition or description. The content may extend to several paragraphs, so observe the opening and closing brackets closely.

- Italicized information in brackets separated by a slash (<*Option 1/Option 2*>) provides two or more policy options that you might consider for your healthcare organization's preferred direction. You can select one or modify a combination and reach consensus on preferred policy guidance.

- A blank line (<_________ >) indicates that you should fill in the blank in accordance with the practice at your organization. This usually designates who or which department performs a typical function or identifies another policy or procedure.

- An underscored area (<*sample*>) indicates that you should fill in the blank—but note the example for clarity.

DOWNLOAD YOUR MATERIALS NOW

Materials available for download upon purchase of this product

About the Author

Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS, is president of Margret\A Consulting, LLC, a firm dedicated to providing effective and efficient solutions to today's information management and systems issues. She also serves on the faculty and board of examiners of Health IT Certification, LLC. She holds an MBA in marketing and finance and a BS in health information management from the University of Illinois at Chicago.

Amatayakul has a long and extensive career history of working in the field of EHRs and associated standards. She has served on the HIMSS board of directors. As the associate executive director of the American Health Information Management Association, Amatayakul was responsible for overseeing academic preparation, continuing education, and certification, as well as the association's early advocacy efforts. Amatayakul has also been an associate professor at the University of Illinois at Chicago and director of health information management at the Illinois Eye and Ear Infirmary. She is currently an adjunct faculty member in the health informatics master's program at the College of St. Scholastica and is on the advisory committee to its Title III grant, which, in partnership with a major EHR vendor, focuses on integrating computer-based clinical information system applications into health sciences professional curricula.

Contributions

Special appreciation to Maria ("Mia") Sakkos for her help in reviewing material for the creation of this second edition. Also, appreciation to Michael R. Cohen of MRC Consulting Group, who contributed to the first edition.

Introduction

The Importance of Policy Directives

Policy is guidance for action that is consistent with legal, ethical, and organizational requirements. Well-written policies establish measurable objectives and expectations, assign responsibility, and define enforcement and consequences for violations. Nearly every organization has policies, even if they aren't written.

This book stresses the importance of written policy in an electronic health record (EHR) environment and helps you create the policies your organization needs to move forward with its EHR initiative. Specifically, this book:

- Underscores the importance of policies in establishing expectations for how staff will use the EHR
- Explains how policies can support the design of your EHR and health information technology (HIT)
- Describes ways policies can aid EHR adoption and realization
- Provides sample templates you can modify to use at your own healthcare organization

The Importance of Policy

Policy is the mutual agreement that outlines the expectations your organization has for its employees and other members of its workforce. For EHR and HIT, policy represents the commitment to install information systems and fully adopt them as intended. Without policy, system implementations will be nonstandardized and defeat their purpose.

A scenario: CPOE

According to a Center for Information Technology Leadership study,[1] half of hospitals indicating they have a computerized provider order entry (CPOE) system require their physicians to use it. The stage 1 "meaningful use" criteria require only 30% of medication orders to be entered by licensed healthcare professionals for physicians or hospitals to earn the incentive.[2] Yet the purpose of CPOE is explicitly designed to support physicians in writing accurate, complete, and legible orders to improve patient safety. Hospitals or clinics that don't require doctors to use CPOE will not see a significant return on investment (ROI) compared to those whose policies require full use. A study recently conducted by the National Academy of Sciences described the EHR and HIT state of affairs as one in which implementations have occurred, but the technology has not been well integrated into clinical practice.[3] There is a big difference between a system that has been implemented and a system that is fully adopted—hence the reason for the incentive program being dubbed "meaningful use."

The following factors contribute to CPOE acceptance and use: corporate culture, engagement of potential users in planning for CPOE systems, acquiring the right system and infrastructure to fully support it, analysis of current and proposed work flows and processes, review and sensitivity setting for clinical decision support, thorough testing, and comprehensive training. Drafting and adopting a CPOE policy is also critical to success and ROI. A lack of policy will affect the broader scope of EHR and all of HIT. Consider the following effects caused by a lack of policy:

> ***Argument:*** Many hospitals will explain the lack of a policy mandating the use of CPOE and other technologies with the excuse that they rely on their physicians to attract patients in a competitive environment and that physicians who are resistant to change or reluctant to adopt new technology will take their business elsewhere.
>
> ***Rebuttal:*** Note that at one time or another, most hospitals have used this excuse to resist other types of change. Generally, hospitals respond slowly but ultimately do adopt the new requirement or technology because in reality, physicians aren't likely to take their patients elsewhere, and "elsewhere" will sooner or later adopt the same type of new program or technology as well. Although this situation may become less common with the advent of the "meaningful use" incentives, there are still many hospitals and clinics that are not sure the incentives are worth the effort. (And whether to seek the incentives is yet another matter for policy deliberation!)
>
> ***Argument:*** Another common excuse for lack of policy is that the CPOE system is new, and the bugs haven't been worked out yet.
>
> ***Rebuttal:*** In this case, the hospital is setting appropriate expectations for neither its physicians nor its staff to ensure the implementation is complete. Without clear

goals and directions, the CPOE implementation could languish for a long period of time without full debugging and adoption.

Argument: A related reason a hospital might cite for not drafting a policy on mandatory use of CPOE is that the hospital may not have fully installed all elements of the system required for its full, optimal use. For example, some hospitals make CPOE available only for ordering medications because communication connections to other systems (to send the orders to), such as laboratory, radiology, nursing service, dietary, and other ancillary destinations, may not exist yet. It is also possible that the full complement of decision support in the system has not been fully built out, so the hospital does not offer the physicians the full value of a CPOE with clinical decision support.

Rebuttal: In this case, the hospital may legitimately recognize that physicians entering orders on the computer to improve legibility is very likely to be perceived as asking physicians to assume clerical functions. In fact, some physicians view CPOE as a way for the hospital to reduce clerical staff.

Clearly, asking physicians to perform clerical functions is not your intent. Keep in mind, though, that it can appear that way if you haven't engaged order sets, templates, and an appropriate set of reminders and alerts to aid the data entry burden and provide visible and important patient safety information. Still, without setting expectations, your hospital may never fully build out the system—or worse, may buy a module without full functionality to respond to pressure from health plans, employers, or accreditation agencies to address patient safety. Once again, your hospital is doing itself a disservice by not making an investment or enforcing a policy that will truly return results.

Establishing expectations

The CPOE scenario emphasizes how important policies are. Policies establish expectations not only for your users, but also for the organization as a whole. In fact, one reason policies are often difficult to write and even more difficult to successfully enforce is that a policy essentially is a contract, or at least a commitment, between two groups or individuals. Those who must comply with the policy often view policies as mandates "from above." Policies can appear to be constraints because they establish boundaries dictating ways people must act. An organization, in turn, may be reluctant to establish a policy if it suspects it may not be able to carry out the policy.

Instead of considering policies from one of those sides, view them as guidance for action based on consensus. While you should lean toward stability in your policies, write policies that allow for flexibility and that leave room for staff members to use their professional judgment when carrying them out. There are three important characteristics to note:

1. Policy viewed as guidance is not constraining. Consider the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA requires hospitals to develop and use policies and procedures to address both privacy and security concerns. However, within the privacy standards, there are 15 references, in seven different standards areas, to applying professional judgment in the carrying out of the standard and their implementation specifications.[4] HIPAA's security policies also recognize the need in healthcare to address emergencies, such as in its emergency access procedure.[5] Clearly, HIPAA legislation recognizes that in dealing with the human condition there can be no absolutes.

2. Policy established through consensus should reflect the interests of all to the extent possible within legal requirements, ethical tenets, and the established organizational mission. Don't decide on a policy without understanding what the policy needs to accomplish and how, together with the staff, you can apply it in a commonsense manner.

3. You may need to update policy as the environment at your organization changes. Reference HIPAA again to establish precedent. Not only does HIPAA legislation allow for change in policies and procedures when necessary,[6] but the Security Rule requires "periodic technical and nontechnical evaluation … in response to environmental or operational changes affecting the security of electronic protected health information (ePHI), that establishes the extent to which an entity's security policies and procedures meet the requirements [of the Security Rule]."[7] The Health Information Technology for Economic and Clinical Health Act of 2009 within the stimulus legislation updates the HIPAA Privacy and Security Rules that must be addressed in organizational policy.[8]

When the individuals who will be governed by a policy invest themselves in creating the policy, they will be more likely to adopt the policy. Revisiting the CPOE example, hospitals that engage their physicians in CPOE planning actually find physicians eager to use the system and address it in the medical staff bylaws.[9] Engaged physicians want to achieve real benefits. The CPOE requirement that the medical staff incorporates into the bylaws, however, should include explicit language to describe the functionality the CPOE system provides and how the medical staff should use the technology. This, in turn, serves as the hospital's goal to provide such functionality by the time the date of the bylaw amendment is effective. See a sample statement below.

Sample Statement of CPOE Use for Medical Staff Bylaws

> Bylaws amendment effective ______/______/______
>
> All members of the medical staff shall place orders for medications and all other services to be performed by hospital staff using an electronic system that supports clinical decision-making. The electronic system will be available at the point of care and remotely, through a secure process. Orders shall be authenticated through the use of an electronic-signature process consistent with legal requirements and as specified in Sec. ______ of these bylaws. Physicians shall be alerted electronically to any order placed verbally with a nurse as specified in Sec. ______ of these bylaws and that requires authentication.

In summary, policy provides a mutual agreement that outlines the expectations for actions within an organization. For EHR and HIT systems, policy represents a commitment to install the system and fully adopt it as intended.

Supporting EHR and HIT Design

Policy that establishes expectations drives EHR and HIT design. Continuing with the CPOE scenario and analyzing the expectations that the sample bylaws amendment establishes, a CPOE system requires the following functionality:

- **Communications capability with all pharmacy, nursing, and other ancillary departments.** However, it is imperative that the hospital is not constrained if a specific ancillary department is not yet automated. Orders placed through CPOE can be printed, faxed, or otherwise transported to that department until the department acquires a system that can serve as an order destination.
- **Clinical decision-support capability within the ordering system.** The sample bylaws amendment does not spell out the level of sophistication for such decision

support. This could be a weakness of the bylaws, or it could be a way for the hospital to develop the sophistication of the decision-support capability over time. How this is actually described in a given set of medical staff bylaws may depend on the level of trust the medical staff has in its hospital, which reflects the degree of involvement of physicians in the EHR system design. In any event, such language allows the hospital to start with a small number of common order sets and drug-allergy/drug-drug interaction checking as a simple type of clinical decision support. Then the hospital can move to more complex drug-lab checking and to using more sophisticated templates.

- **Point-of-care availability.** Again, the bylaws do not spell out the exact nature of the input devices. For example, nowhere in the bylaws does it say that every physician will be issued a device. Instead, the language implies that technology will be convenient and devices ubiquitous. This language gives the hospital leeway to work with the physicians to determine what is best and also allows for change over time as new technology emerges.

- **General availability.** Availability generally refers to the likelihood that systems are able to function properly so providers can continuously administer care. This may include drafting a policy to address server and network redundancy to ensure that there is virtually no downtime.

  Note: One might argue that this concept of availability is inherent in the statement because no provision is made for reverting to paper order writing. However, this may be too strict an interpretation for others to make. Again, the degree of specificity may have been left to "professional judgment" due to the quality of the medical staff relationships, or it could be an oversight in writing the amendment.

- **Secure remote ordering capability.** This is an important functionality that can reduce errors associated with verbal orders. On one hand, it demonstrates the medical staff's commitment to making CPOE work. On the other hand, there may be some appropriate qualifications to add to reduce the risk of physicians writing orders based on Web-based information without actually visiting the patient.

- **Electronic authentication.** The sample bylaws amendment suggests that such functionality apparently already exists, probably for dictated reports. It is important for the bylaws to recognize, however, that legal requirements related to certain kinds of medication orders may exist. Again, the hospital should not be constrained by any specific type of authentication.

- **In-basket or deficiency notification.** This functionality ensures that doctors authenticate verbal orders in a timely manner. This implies the system is more than merely a provider portal for the physician to visit periodically to place orders and retrieve results. The alerting or notification functionality implies that there is a system that pushes an alert or notification to the physician. For example, there could be an in-basket function that appears each time the physician logs on to the hospital's computer system, an alert transmitted via a pager, or even an alert transmitted into the EHR at the physician's office. Again, the language in this sample bylaws amendment allows for flexibility as the hospital acquires more technology.

Although the sample bylaws amendment directly describes these functions, there are many other functions that a CPOE system could incorporate. You can address these in other policies. For example, you can include CPOE functionality in your Joint Commission requirements for medication management and improving organizational performance.[10] CPOE is also not the only technology that addresses patient safety. The Joint Commission's Sentinel Event Alert, Issue 42, highlights barcode medication administration record systems as well as CPOE systems.[11]

In summary, policy should be sufficiently specific to support EHR and HIT design, while not encumbering your organization by forcing it to acquire certain functionality that could be impossible at this time or limit future progress.

Improving Adoption and Benefits Realization

Despite the growing momentum for EHR and HIT and the recognition that technology is very rapidly becoming part of the cost of doing business in healthcare today, healthcare executives still are greatly concerned with their cost and their ability to make a real difference. Many healthcare executives question the ROI of an EHR and other HIT. Policies that guide EHR design and establish expectations can improve the adoption of the systems and the realization of benefits.

ROI versus the benefits portfolio

There are many concerns surrounding the ROI of EHR and HIT. For instance, a pure financial ROI is often not possible or even expected from EHR and HIT. Instead, many healthcare executives are willing to accept a benefits portfolio of both financial and quality benefits. However, the benefits portfolio must be quantifiable.

For example, a hospital will want to know whether its CPOE system is actually reducing ordering errors. The challenge, of course, is to have sufficient benchmark data available to make a comparison. Do you know how many errors occur in the ordering process? Do you need to conduct a formal study to determine a benchmark? Is your hospital willing to conduct such a formal study? If so, the study itself is an added cost to the overall system. If not, and the administration takes it on faith that improvements are occurring, you won't have evidence to substantiate or refute a challenge that CPOE appears to be making no difference. There is less incentive for those resistant to change to adopt a system if you can't prove that it makes a difference.

Some hospitals rely upon adoption rates as surrogates for benefits and determine how many unique user logons occurred each day. Adoption rates alone, however, are insufficient to determine how effective CPOE use is. Consider that near 100% CPOE adoption could, in fact, have no impact on patient safety. In many cases, the impact depends on the incremental changes to current practices. If current practices are strong, the incremental differences will not be great.

Still, most hospitals that have had success with CPOE and other EHR and HIT initiatives believe it is very important to conduct a benefits realization. In itself, feedback on improvement can be a great motivator and keep compliance high. For CPOE as an example, hospital pharmacies may track the number of illegible orders they receive. Illegible orders have become such a serious matter that Montana actually made it a civil offense for any medical provider to write an illegible prescription (see the new prescription law on the next page). Another benchmark might be the number of calls made by pharmacists to physicians about potential drug contraindications.

When developing policies for EHR and HIT, you should incorporate a feedback mechanism that describes why the policy is important.

New Law Requires Legible Prescriptions

The Montana legislature passed a law, effective October 1, 2005, declaring that it is a civil offense for any medical provider to write an illegible prescription. Patients can file complaints about illegible prescriptions with the practitioner's licensing board. Licensing boards can decide whether to investigate, impose sanctions, or turn cases over to county attorneys for prosecution. If a case is successfully prosecuted, the physician can pay up to $500 in fines for each illegible prescription.

Many look-alike and sound-alike drug names have prompted this action. For example,

- Zyrtec, an antihistamine, was dispensed instead of Zyprexa, an antipsychotic
- Toprol, a medication to lower high blood pressure, has been confused with Topamax, used to treat seizures
- Lamisil, an antifungal medication, has been mistaken for Lamictal, a mood stabilizer and anti-epileptic

Source: Billings, MT, Gazette, October 22, 2005.

Intervening variables

Another concern surrounding ROI related to computerization is the fact that EHR and HIT take a long time to implement, and hence there are many intervening variables that may contribute to or detract from achieving an ROI. It could take several years to automate sufficient source and destination systems that fully realize CPOE's potential. It could take several more years for the CPOE system to be fully built, with all order sets, templates, and decision-support rules fully designed, tested, and adopted. Policies that incorporate feedback to demonstrate benefits must recognize the potential for intervening variables. Stating that using CPOE should "contribute to" patient safety is better language than stating that CPOE "will result" in patient safety.

ROI beneficiaries

Finally, some industry leaders believe that the primary beneficiary of EHR and HIT is neither the patient nor the healthcare organization or provider—but the insurance plan.[12] If electronic entry takes the physician several seconds longer than a paper order, and the physician thinks the primary benefit of CPOE is to lower the cost of drugs for health plans, the physician will thoroughly resent those additional seconds.

The value of CPOE (or any component of EHR and HIT) must translate into value to the patient and, if possible, value to the provider as well. Many providers think entering data into an EHR takes longer than doing so on paper, and they often overlook the downstream time savings from better documentation. It is important to demonstrate that such additional effort can result in eliminating phone calls about potential drug contraindications, duplicate lab tests, lack of diagnoses for medical necessity, and other problems associated with incomplete, inaccurate, or illegible documentation. In an office setting, the capture of more complete and structured data significantly reduces transcription expense and abstraction expense (if the office is participating in a disease registry) and provides better data for patient treatment.

Of course, you should make an effort to implement systems to reduce the actual data entry burden as well. For example, EHR and HIT can support patient entry of medical history via a context-sensitive automated medical history system;[13] medication history can be compiled from claims data supplied by a consolidator such as RxHub;[14] and well-designed templates with data entry aids and embedded decision support[15] can significantly reduce the time it takes to enter data.

Policies that suggest that the organization and not the patient or user is the beneficiary are less likely to support compliance.

In summary, it is important to have well-written policies with input from all who will be affected by them. Policies that establish expectations can support EHR and HIT design and help achieve adoption and benefits realization.

References

1. Center for Information Technology Leadership. "The Value of Computerized Provider Order Entry in Ambulatory Settings." Executive Preview, 2003, p. 2.

2. 42 *CFR* Parts 412, 413, 422, et al., Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule, July 28, 2010.

3. Stead, William W., and Herbert S. Lin, eds. *Computational Technology for Effective Health Care: Immediate Steps and Strategic Directions.* The National Academies, 2009. Available at *www.nap.edu/catalog/12572.html.*

4. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996, Standards for Privacy of Individually Identifiable Health Information §164.502(g)(1), §164.510(a), §164.510(b), §164.512(c), §164.512(f), §164.514(h), §164.524(a).

5. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996, Security Standards for the Protection of Electronic Protected Health Information §164.312(a)(2)(ii).

6. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996, Security Standards for the Protection of Electronic Protected Health Information §164.316(a), and Standards for Privacy of Individually Identifiable Health Information §164.530(i)(2).

7. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996, Security Standards for the Protection of Electronic Protected Health Information §164.308(a)(8).

8. 45 *CFR* Parts 160 and 164, Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, July 14, 2010.

9. Laughlin, J., and J. McGuinness. "Successes and Challenges for HIM and Physicians in CPOE." Watertown Area Health Services, presentation at the Wisconsin Health Information Management Association, March 17, 2006.

10. The Joint Commission. Medication Management (MM) Standard MM.08.01.01 and Improving Organization Performance (PI) Standards PI.03.01.01. *Comprehensive Accreditation Manual for Hospitals: The Official Handbook,* updated July 26, 2010.

11. The Joint Commission. Sentinel Event Alert Issue 42: Safely Implementing Health Information and Converging Technologies, December 11, 2008.

12. Chesanow, N. "EHRs: Where Do Payers Fit In?" The Connected Physician, "Special Technology Section," *Medical Economics,* February 17, 2006.

13. Bachman, J. "Return on Investment From Using Instant Medical History™." Department of Family Practice, Mayo Clinic, November 2002.

14. Fischer, Michael A., et al. "Effect of Electronic Prescribing With Formulary Decision Support on Medication Use and Cost." Press Release, December 9, 2008, Agency for Healthcare Research and Quality. Available at *www.ahrq.gov/news/press/pr2008/eprescribpr.htm*.

15. Chin, H.L. "The Reality of EMR Implementation: Lessons From the Field." *The Permanente Journal* 8(4), Fall 2004.

CHAPTER 1

Creating Policies

It's important to write effective policies that support the adoption of electronic health records (EHR) and health information technology (HIT). Written policies must be carefully crafted to ensure staff compliance.

This chapter provides guidance in writing effective policies that will help your organization make appropriate decisions. This chapter also acknowledges the challenges in creating policies absent legal or regulatory guidance. Specifically, this chapter:

- Defines "policy"
- Defines the legal basis for policy
- Distinguishes policy from procedure and standard
- Describes the policy design process
- Offers tips for drafting effective policies
- Provides aids to obtaining approval for policies
- Suggests ways for gaining acceptance of policies
- Presents ideas for monitoring compliance with policies

Policy Defined

The *Random House Webster's College Dictionary* defines policy as a "definite course of action adopted for the sake of expediency." It further suggests that a policy describes the prudent action to take. *Merriam-Webster's Online Dictionary* defines policy as a "definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions." It also describes policy as a high-level overall plan embracing the general goals and acceptable procedures, especially of a governmental body. Finally, the SysAdmin, Audit, Network, Security Institute (SANS), a source for information security training and certification, offers a security policy framework that applies to EHR policies. It notes that policies:

- Define appropriate behavior
- Set the stage in terms of what tools and procedures are needed
- Communicate a consensus
- Provide a foundation for human resources action in response to inappropriate behavior
- May help prosecute cases[1]

Dissecting these definitions offers important insights into elements of policy.

Address expediency and prudence

A policy must be expedient—that is, convenient, practical, useful, and appropriate. It must also be prudent—that is, careful, cautious, discreet, and sensible.

In the context of EHR and HIT policies, these concepts make a lot of sense. Your policies should not require action that is difficult or a hassle for your staff to perform but should reflect what is right for your organization and its mission. For example, consider your access control and authentication policies and how you could revise them to support the design of EHR and HIT. They should:

- Ensure that the appropriate staff members can access needed information but also restrict access to or action by unauthorized staff members.
- Be sufficiently flexible so that in an emergency situation you can authorize access for different clinicians or staff members. For example, a nurse who is normally restricted to accessing patient information on an assigned nursing unit may need to access information for a patient on another unit in the case of a life-threatening event.
- Ensure the confidentiality, integrity, and availability of data so you can determine the legitimacy of an employee's access/action.
- Be easy to use. For example, you may not want to require users to remember multiple layers of complex passwords that change every 30 days. Instead, you may want to consider single sign-on technology to manage appropriate levels of access.

Determine action from possible alternatives

In healthcare, the appropriate action to take is rarely completely clear. Because policies guide action, policies come in handy when there is a potential for alternatives—especially when some alternatives are more expedient than others.

Legal basis for policy

The idea that the appropriate action to take is rarely completely clear in healthcare is also very true in the field of information technology. As organizations approach the use of EHRs, there will be many dilemmas. While there are many examples, two serve to illustrate this issue: Will documentation aids that make it easier to gain user adoption hold up under scrutiny by The Joint Commission or in a court of law when their results make every record look similar? Must the rationale for overriding an alert be documented in an EHR when such rationale was rarely documented in the paper chart?

Policy is guidance for action that is consistent with legal, ethical, and organizational requirements. Unfortunately, for many of the issues associated with EHRs, there are yet to be laws, regulations, or statutes that provide definitive answers. In fact, law almost always lags behind technology. So, while your policies must conform to applicable federal and state laws, regulations, and standards and the requirements of licensing and accrediting agencies, in their (frequent) absence, your policies need to reflect the mission and culture of your organization, codes of professional conduct, best practices offered in peer-reviewed publications, task forces of experts, and the ethical principles espoused by your organization. Your policies should guide your staff to make expedient and prudent decisions within such context. (See **Figure 1.1**.) It is very likely that enhanced information technology (IT) use will continue to provide challenges to your current policies and also open new areas for policy development.[2]

In summary, policy guides decision-making, provides a frame of reference for action, establishes goals that procedures and technical measures serve, and sets rules for disciplinary action.

FIGURE 1.1 Three Ethics Principles to Help You Draft Policies

The Belmont Report[1] provides a basis for ethical decision-making in healthcare. It describes three basic principles that you should keep in mind when drafting policies:

1. **Respect** means that individuals are autonomous, capable of deliberation about personal goals, and able to act under the direction of such deliberation. It also supports the concept that persons with immature or diminished autonomy are entitled to protection. Every day, healthcare professionals apply professional judgment when making choices. For example, physicians must decide whether to administer a medication in an effort to improve a patient's condition if there is evidence that the patient has hypersensitivity to its active ingredient.

   EHR and HIT further enhance decision-making with reminders, alerts, and knowledge sources. Clinicians and staff members will continue to make and document decisions. Consider how a court of law will interpret documentation if an action prompts legal consequences. You will also need to determine how to document an unusual circumstance.

2. **Beneficence** refers to acts of kindness or charity that go beyond strict obligation. More than "do no harm," a well-known fundamental principle of medical ethics, beneficence implies that professionals should "maximize possible benefits and minimize possible harms." EHR and HIT go hand in hand with beneficence because they represent an effort to improve patient care and customer service.

   Beneficence relates to the construction and support of EHR and HIT. It's the difference between merely acquiring basic computing technology and choosing a system and providing staff training to meet sophisticated standards. It's also important to remember that acquiring an EHR system without sufficient technical infrastructure (and financial support) will result in slow, cumbersome systems that experience extensive downtime. Doing so puts patients at risk because clinicians won't adopt the awkward system, and your facility won't be using its resources effectively.

3. **Justice** means treating others fairly. In healthcare, justice refers to the distribution of benefits or allocation of risks. Some industry leaders think that all who benefit from EHRs—meaning policymakers, employers, payers, researchers, and educators[2]—should share the costs. Providers may also question justice during EHR and HIT adoption. For example, physicians might ask, "I was not involved in the choice of this system, so why should I use it?" or say, "I'm uncomfortable using a computer in front of my patients, so I don't plan on using it at the point of care." Therefore, it's important to incorporate the ideas and feedback from system users.

References

1. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, National Institutes of Health, Office of Human Subjects Research, "The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research," April 18, 1979.
2. Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care,* Second Edition, Edited by D. Detmer, R. S. Dick, and E. B. Steen, Washington, D.C.: National Academies Press, 1997, pp. 149-150.

Resources:

1. Fleming, David A. Chapter 14: "Ethics Conflicts in Rural Communities: Health Information Technology," Trustees of Dartmouth College, Hanover, NH, 2009. Available at http://dms.dartmouth.edu/cfm/resources/ethics/chapter-14.pdf, accessed August 28, 2010
2. Mercuri, John J. The Ethics of Electronic Health Records, Clinical Correlations, The NYU Internal Medicine Blog, January 15, 2010. Available at http://www.clinicalcorrelations.org/?p=2211, accessed August 28, 2010.

Policies and Procedures

Policies guide action; procedures direct action. Policies are broad, high-level statements or even plans that document directives. Policies are corporatewide. They require approval from executive management and reflect the overall position on organizational issues.

Procedures provide explicit, step-by-step instructions employees should take to follow policy. Organizational units or departments can modify procedures as they see fit. Procedures may need only middle-level management approval. Procedures, however, must not change the intent of policy. Procedures, with respect to an action, explain:

- What to do
- When to do it
- Where to do it
- Who should do it
- Exactly how to do it

Figure 1.2 provides an example of a policy statement and related (part of a) procedure. This figure demonstrates that the policy is a broad statement addressing a specific action where there could potentially be at least two alternatives: use of a secure portal or use of e-mail over the open Internet. The procedure is much more specific, such as describing how an individual may acquire a user ID and password to access the secure portal.

This policy and its related procedural components also illustrate a fairly restrictive model. If this were an actual policy, it would be interesting to know the following:

- Does an employee actually monitor e-mail?
- How is protected health information (PHI) detected?
- Will management enforce the policy with consistent disciplinary action?
- Will management allow any exceptions—for example, if access to the portal is down?

Policies are rarely effective if they are too restrictive. They are also ineffective if management does not monitor policy use and apply incorporated sanctions consistently.

FIGURE 1.2 Policy vs. Procedure

Policy	Procedure
To protect our patients' confidentiality, staff members must send electronic communications containing PHI only via the organization's secure portal. The organization will monitor e-mail sent over the open Internet for PHI and conduct disciplinary action against senders who violate this policy.	1. Individuals must be authorized to receive credentials for using the organization's secure portal for communications with patients: a. Clinical staff members who have reason to use the secure portal for patient communications must present an authorization from their department manager to obtain a user ID and password, which must be changed quarterly. This access is available only within the secure network of the hospital. b. Members of the medical staff who request remote access to the portal will be assigned a secure token upon appointment, which they must renew each time they are recredentialed. 2. To obtain credentials, all users must present a government or organization-issued photo ID to the system administrator. Users must complete an online training program on acceptable use of the Internet and use of the secure portal within three days of receiving their credentials, or the credentials will automatically expire.

Policies and Standards

In many cases, policies (or procedures) reference standards, which provide specifications for action. Your policies should either specify standards directly or imply reference to such standards (which your procedures should detail).

For example, your policies for privacy, security, and transactions and code sets should reflect standards in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) component of the

American Recovery and Reinvestment Act that enhances the HIPAA Privacy and Security Rules. However, the policies should also specifically describe how your organization intends to carry out the standards.

Even though HIPAA references very specific standards for the transactions and code sets rule, the law still provides some leeway. For example, your organization can choose to use a clearinghouse to convert nonstandard claims to standard claims for transmission to payers. Your organization can also choose to adopt the eligibility inquiry and response transactions (ASC X12 v4010 270/271)—or you may decide to rely on direct data entry to access eligibility information from a payer's website. As time goes on and the standards are updated, your policies may change as well. For instance, with the requirement to adopt ASC X12 v5010 by January 1, 2012, hospitals may decide it is more cost-effective not to use a clearinghouse for claims. Your hospital may also have added much more IT infrastructure such that real-time eligibility verification will allow it to improve collections and reduce denials.

The following additional standards development organizations are identified in the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule.[5] Standards from the following organizations enable EHR technology to be certified so that providers may earn incentives for meaningful use of EHRs:

- Health Level Seven (HL7) enables exchanging health information among applications within an organization and exchanging health information with other organizations
- National Council for Prescription Drug Programs (NCPDP) enables electronic prescribing (eRx)
- Digital Imaging and Communications in Medicine (DICOM) provides standards for the exchange of clinical images in picture archiving and communication systems (PACS)
- ASTM International provides the Continuity of Care Record (CCR), which is the data set to be used for patient summary records
- The International Health Terminology Standards Development Organization (IHTSDO) is now the standards development organization that has authority over

maintaining SNOMED CT that is identified in the meaningful use regulations as an alternative vocabulary for encoding problem lists

- Logical Observation Identifiers Names and Codes (LOINC) produces a vocabulary standard for sharing laboratory and other observational data, such as vital signs and history and physical exam information
- RxNorm provides normalized names for clinical drugs and links its names to many of the drug vocabularies commonly used in pharmacy management and drug interaction software, including those of First Databank, Micromedex, MediSpan, Gold Standard Alchemy, and Multum
- International Classification of Disease (ICD) is considered a standard for encoding problems and diagnoses
- Procedure Coding System (PCS) and current procedural terminology (CPT) are standards for encoding procedures for hospitals and physicians, respectively
- The National Institute for Standards and Technology (NIST) and Federal Information Processing Standards (FIPS) contribute security standards for certified EHR technology

The federal government and standards-setting organizations aren't the only bodies that can promulgate standards. Certain "best practices" stem from professional associations or societies. For example, the American Health Information Management Association (AHIMA) released a practice brief on patient anonymity to establish a language standard (e.g., undetermined, good, fair, serious, or critical) that hospitals should use in a policy and procedure about releasing patient information to the media. AHIMA's brief, along with a similar statement from the American Hospital Association, has emerged as the standard of practice. AHIMA has also established the standard concept of the legal health record for providing healthcare organizations guidance on what information from an EHR should be released upon subpoena for a "complete" medical record.

Figure 1.3 summarizes the distinctions between policies, standards, and procedures, as well as methods, which are yet another element of action—rarely codified in written documentation but important in how staff members perform their daily tasks.

FIGURE 1.3 Action Directives

- *Policies* provide overall guidance for expedient and prudent action. They answer the question, "What should be done?"
- *Standards* are, by authority, formal consensus, or by default, rules or frameworks for specific elements of action.
- *Procedures* are specific steps used to carry out an action as specified in a policy and/or a standard. Procedures answer the question, "How should this be done?"
- *Methods* are ways employees actually carry out procedures for a given action, especially where variability is permitted.

Policy Design Process

Follow a formal process to create all policies at your organization. Your policy design process should specify:

- Who develops the initial draft of the policy
- What elements a policy must contain
- Which groups will review each policy
- How the approval process works
- How you will implement the policy

Sources of policy

Although there will likely be a policy development team that drafts needed policies, there should be an identifiable source for each policy. In other words, policies should be driven by a specific need. Any staff member who recognizes a need for a policy or modification to a policy should feel encouraged to submit a policy idea for consideration to your organization's policy development team. In fact, if your organization can cultivate such policy generation, employees will probably consider the organization a good place to work.

Policy ideas for the EHR may be generated by the team that is planning for and implementing the system. Of course, many EHR-related policies will come from new regulations and technology.

For example, an application analyst might notice the need for consistent screen layouts, especially check boxes and radio buttons. This may seem like a trivial matter not worthy of policy. However, inconsistency in how users enter data can cause confusion and result in erroneous data entry, further contributing to—rather than solving—patient safety and quality problems. To address the analyst's concern, your policy could require the use of "standard visual representations" as a general directive encompassing all aspects of screen layout design rather than state "use check boxes when any number of choices may be selected and use radio buttons when choices are mutually exclusive."[3] No matter how strict you make the language, policy needs to guide EHR and HIT design to guarantee data quality.

When users request guidance on legal, ethical, or organizational issues relating to EHR and HIT, be aware that such questions could lead to potential policies. Reference policies when users ask such questions to ensure that a policy that provides direction actually does exist. If not, create one.

Good examples of requests that may come to the policy development team include those surrounding acceptable use of information system assets, e-mail, and the Internet. Most recently, healthcare organizations have been challenged to think about policies for use of social networking media. Such increasingly prevalent issues point to the fact that policy needs to be thoughtfully considered. A policy that simply states you must never do something, such as remove laptops from the premises, e-mail patients, use the Internet to download freeware, or use social media, will not only be disliked but most likely never followed. It is by far better to put appropriate controls around their use and provide education on best practices for their use.

Policy development team

Your organization may already have organizational units that serve as policy development teams. If your organization is large enough to have many, each team is probably specific to whom the policy governs. For example, you might have a team to represent the medical staff—probably the medical staff bylaws committee or medical record committee. Other common teams that generate policies are IT steering committees and health information management (HIM) committees.

The purpose of the policy development team is to:

- Draft policies to respond to the needs of your organization
- Create an inventory of current policies
- Take a proactive position on identifying new policies or needed modifications to existing ones

Organizations that strive to engage the right people in the design of policy will have much better success in their compliance. Because the EHR crosses all disciplines and will reduce the information silos in most hospitals and other large healthcare organizations, a cross-cutting, multidisciplinary policy development team will be the most beneficial. Although a very large team gets unwieldy, advisors, *ex officio* members, and even subcommittees can help maintain order. Include the following on your policy development team:

- An executive sponsor, a member of executive management who can help ensure that your organization's culture and strategy is reflected in the policies. The executive sponsor can then help promote approval when policies reach executive management.
- Representatives from both the leadership and user communities in the medical staff, nursing services, ancillary services, patient financial services, HIM, and IT departments.
- Privacy and security official(s). They should serve regularly or as *ex officio* members because so many EHR and HIT policy aspects touch on protection of confidentiality, data integrity, and system availability. Privacy and security policies already exist at your organization, and you can probably enhance the existing policies to reflect EHR and HIT rather than create new ones.
- Legal, risk management, and medical staff credentialing advisor(s).
- A technical writer, to draft policies that are concise and easy to understand.

Drafting Policies

Some policy changes you need to make are obvious. However, to cover all of your bases and make sure you comprehensively update policies across your organization, take stock of what policies already exist and what policies you need.

Step one: Take a policy inventory

Ensure that your organization's policies are EHR-ready by taking an inventory of existing policies that relate to all aspects of information management. It is very likely that your HIM department has a list already or is a good place to start to compile the list. Also check for an inventory compiled for a HIPAA privacy and security assessment. **Figure 1.4** provides a sample policy inventory with some examples to illustrate each of the components of the inventory tool. Once you inventory current policies, your policy development team should work backward and make a list of all effects EHR and HIT may have on existing policies. You can use the policy inventory and work from right to left, rather than left to right (see Figure 1.4). Use the inventory as a checklist to update all policies that will need to change as HIT becomes prevalent throughout your organization. The Joint Commission accreditation manuals are good resources to address all aspects of information management.

FIGURE 1.4 **Sample Policy Inventory**

Policy number	Policy title/focus	Internal source	External reference	Date created	Revision history	Policy owner	EHR/HIT impact
ITS 201	Access controls	IT	HIPAA ISO17799	March 4, 2003	April 16, 2010	ISO	Needs "break the glass" (BTG) for emergency access
HIM 098	Medical record retention	HIM	AHA state statutes	Jan 1, 1975	1982 1996 2003 2009	HIM	Needs revision for paper copies as EDMS is adopted and as EHR will be adopted
Medical Staff Bylaws Sec. 042	Electronic authentication of documents	MRC	HIPAA	July 1, 1995		HIM	Extend to all components of EHR
IM 502	Medication history	EHR	MMA	2003	2008	Pharmacy	External sources of medication history
IM 512	Clinical decision support alert override	EHR	HITECH HIT standards	July 2010		CMIO	Documentation of rationale for overriding clinical decision support

Source: Copyright ©2010, Margret\A Consulting, LLC.

Step two: Include essential policy elements

Policies must be enforceable. They must also be concise and easy to understand—while balancing expediency and prudence. For example, a security policy should balance protection with productivity. An information retention policy should balance cost, patient readmission or revisit rate, research interests of the organization, and other internal requirements with state statutes of limitations.

Policies should incorporate the reason(s) your organization needs them, describe what action(s) the policies cover, define responsibilities, and discuss how management will address violations. Include the following basic elements in your policies:

- Title—should be short but descriptive to uniquely identify the document.
- Purpose—to state the reason the policy exists.
- Policy statement—the specific guidance for action, including measurable objectives and expectations, responsibility, enforcement measures, and consequences for violations. Sometimes each of these elements will appear in separate sections of the policy document.
- Effective date.
- Review/revision date.

Never destroy policies. Even if a policy is no longer applicable, retire it and place it in a permanent file. It may be necessary in the future for your organization or an employee to prove that a previous action was or was not consistent with an old policy.

Step three: Consider optional components

In addition to the essential policy components, you may want to include the following elements in your organization's policy documents:

- Policy number—an indexing mechanism for your organization
- Page numbers—to ensure employees consider a multipage policy in its entirety
- Scope—a description of to whom the policy applies and/or circumstances for its use
- Related policies—for convenience in the event that two closely related policies exist
- Definitions—any terms included in the policy that are unique or could be misunderstood

- References or sources of policy directives—specific regulations, accreditation requirements, or other standards that specify the source of direction, the legitimacy of policy content, or evidence that the policy is appropriate guidance
- Authority and approval—the title and signature of the executive or officer who approves the policy
- Policy owner—the title of the person who would most likely manage policy revisions
- Rider—to authenticate the receipt of and the agreement to abide by the policy directive

Because policies must be concise and easy to understand, they should be no longer than two pages. If your policies have a tendency to run long, it is likely that you are actually developing a procedure. In this case, you may want to set aside the document and review it again later to cull out only the who, what, and why. Leave the how for the procedure.

Step four: Write policy statements

The policy statement itself is the most important element of the policy document. Take the following steps to create an effective policy statement:

1. Understand the circumstances pertinent to the policy you are writing. For example, you may need to read your state's statute of limitations, an EHR documentation manual, applicable case law, applicable standards, the HIPAA Privacy and Security Rules, Medicare *Conditions of Participation,* current literature, or any other material that would establish a solid background for policy writing. You should also fully understand how the EHR works and how the staff will use it. Discuss its components with users and the IT staff.
2. Determine your organization's corporate position relative to the policy. You need to verify whether staff members are presently following the requirement for which you are writing the policy. If not, consider the possible reactions in the areas the requirement will affect. Understanding your organization's mission, EHR vision, strategic initiatives, and other corporate culture resources can help clarify the appropriate direction for the policy.

3. Draft the policy to reflect your organization's culture and meet corporate expectations for EHR use and EHR functional and technical capabilities.

4. Test the draft of the policy on individuals who will eventually adopt and enforce the policy. Ask for their feedback, concerns, and questions. Then return to the policy development team to further discuss and address the feedback.

Policy templates

A policy template is a pattern or example of what a policy on a specific topic should (or could) include. A policy template provides sample language. It may help identify all possible alternatives.

A template is a good way to start developing your policies. Remember, however, that policies are very specific to the organization and its culture. EHR and HIT policies require you to be even more specific to reflect your technology's capabilities.

Policy statement example

Sample **Policy 1** is on an individual's right to request restrictions on information use and disclosure. It reflects what many organizations adopted under the HIPAA Privacy Rule when protected health information was primarily in paper form. The sample Policy 1 can be found at the end of this chapter.

This sample policy:

- States the source of the policy (the HIPAA Privacy Rule)
- States the purpose (to fulfill the requirement for individuals to be able to request restrictions)
- Identifies who is responsible to carry out the policy
- Describes what actions employees must take
- Establishes that the information privacy official will enforce it
- Describes consequences for violations that are consistent across all potential users of the policy

This policy, however, is quite restrictive, suggesting that it will be very difficult to accept most requests. As HITECH encourages more data protection and requires acceptance of restrictions on releasing information to insurance companies for cash-only patients, organizations will need to not only update their policy on restrictions but find technical ways to ensure such restrictions can be accommodated. This is also a good example of the need for a cross-cutting stakeholder team. Once more and specific access controls and better audit logging exist, some of the restrictiveness of this sample policy should be tempered.

To test a revision to the policy, take the following steps:

1. Ask those who use the policy to review and comment on how they use the policy. For example, ask patient access staff how many requests for restrictions they currently receive. Determine whether they understand the policy's objectives and who is responsible for enforcing the policy.

2. Obtain scenarios from healthcare professionals concerning potential policy directives, such as when it's appropriate for individuals to ask for restrictions.

3. Draft a revised policy and test it against the scenarios.

4. Draft procedures associated with the new policy to determine whether the policy directs every step. In the case of the policy on restrictions, draft the procedures for patient access staff members to refer requests and for healthcare professionals to take action on the requests. Then determine whether the revised policy directs every step.

5. Test the potential new policy with your organization's IT test or development environment. This will ensure that the policy works but does not disrupt the production environment if there is a problem with the policy execution. For example, for restrictions, test the flow of information on which there is a restriction and determine whether you can manage it at every point, from patient registration/admission through billing and permanent disposition.

6. Redraft any part of the policy that fails these tests.

Testing a policy ensures that it is clear and concise, that procedures can support it, and that it will actually work.

Approval Process

In most organizations, executive management must approve policies. Executive managers may not need to understand every nuance of EHR and HIT policies (which tend to be complex), but you do need to inform them about why the policy is necessary and assure them you have thoroughly reviewed and tested the policy.

Executive management may also want to understand the effect the policy has on your organization:

- Whom will the policy affect?
- Will the policy result in a positive or negative change?
- Who will be happy? Who will be unhappy?
- Will implementation result in new and direct costs, additional time, or cost/time savings?

In a way, this process is similar to that of conducting a HIPAA risk analysis and providing executive management with information about the level of residual risk inherent in the policy. Residual risk is the amount and type of risk that remains despite implementation of a policy.

Include a cover memo with the policy when you submit it to executive management for approval. Provide the following information:

- Summary of the policy
- Reason for the policy
- Description of the impact
- Risk assessment

Policy risk assessment

Any policy carries the risk of being too lenient or too severe, being misunderstood, or negatively affecting one area while positively affecting another. An example is a very conservative policy on accepting restrictions in only certain, special circumstances, which:

- Minimizes risk associated with not having information for treatment and lessens the possibility of violating a restriction
- But may increase the risk of unhappy patients who may file complaints and lower patient satisfaction scores

With respect to risk, executive management needs to understand:

- The probability of the risk threat occurring (e.g., more complaints)
- What impact the threat may have (e.g., a federal government investigation)
- What costs or other resources would be required to reduce that risk further

Once risk is clear, executive management can either:

- Accept the residual risk proposed (and hence the policy)
- Apply more resources to reduce the risk further (requiring a modification of the proposed policy)

Gaining acceptance of policy

Just because executive management has approved a policy does not necessarily mean the staff will accept and use the policy. Respond to problems with a willingness to address them in an additional policy, develop consensus on the direction the policy should take, engage all appropriate persons in the drafting and testing of the policy, and conduct an appropriate risk assessment. The most important success factor is engaging the staff members who will need to follow the policy in the full development process.

Note that the policy elements in this chapter include both enforcement measures and consequences for violations. Sometimes these terms are interpreted to have the same meanings. There is an important distinction, however:

- Enforcement measures describe how policy enforcement will happen. In the case of the sample policy on restrictions, the information privacy official who receives a copy of all requests and reviews them for compliance carries out enforcement.
- Consequences for violations are the actions your organization will take if your enforcement mechanisms determine that an employee that has violated the policy.

Staff members are more likely to accept policies that your organization visibly enforces. For example, if staff members see that there is zero tolerance for accessing the records of a patient with whom they do not have a specific work-related relationship, it is very likely that they will adhere to the policy rather than risk termination. However, if no sanctions for such action are visible or applied inconsistently, staff members may not consider the policies very important and, worse, could file for discrimination if policies are applied to them and not to others. As regulations forthcoming from HITECH step up provisions for HIPAA enforcement, increased amounts of civil monetary penalties, and clarification that HIPAA penalties can be levied on individuals, there will very likely be the need for review and improvement of policies and their enforcement.[4]

In addition to engaging individuals in policy setting and visible enforcement, many healthcare organizations use a layered approach to ensure they communicate policies (and procedures) to all members of the workforce:

- Education is classroom instruction. Virtually all workers will need to learn about EHR and HIT policies.
- Training is on-the-job skill building. Many potential users of EHR and HIT will require intensive training on specific policies to be able to use EHR and HIT.
- Awareness provides ongoing reminders to maintain compliance. These reminders may include reference material, intranet sites with policies and procedures, a glossary of terms, and information system pop-ups.

In whatever manner individuals learn about policies in the organization, you need to inform them about:

- Where they can reference policies
- Who can answer their questions
- How policy compliance affects their performance evaluation
- What sanctions are associated with a violation of policy

Ongoing Compliance

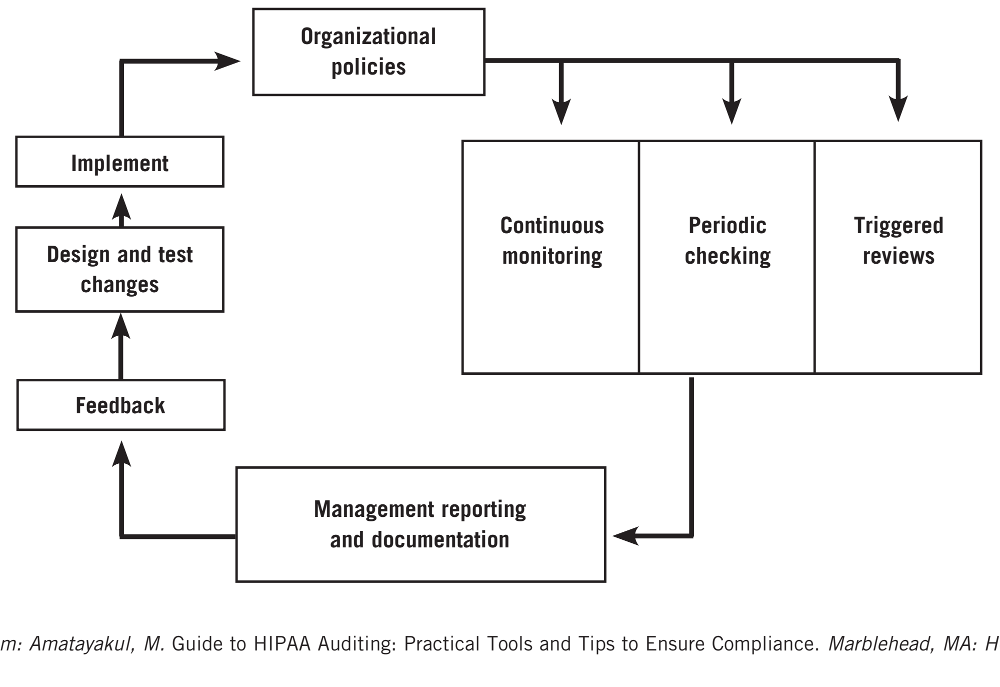
The purpose of policy is to ensure that your organization manages its business consistently. Policies must cooperate with the organization's leadership principles, style, culture, and directives. To be truly effective, you and your organization must apply policies in the same manner so you always reach the same conclusion.

In addition to providing direction on how to act, use policies to evaluate those actions and identify corrective measures if necessary.

Policy development is not the end—but the beginning—of an ongoing compliance assurance system. A feedback mechanism describes how organization controls described in the policy can be applied to monitor, report, get feedback, and make changes. See **Figure 1.5**.

In summary, the policy design process should help you develop policies that work. It balances all aspects of organizational requirements to ensure appropriate expectations and the realization of benefits.

FIGURE 1.5 **Feedback Mechanism**



Adapted from: Amatayakul, M. Guide to HIPAA Auditing: Practical Tools and Tips to Ensure Compliance. *Marblehead, MA: HCPro, Inc. 2004.*

References

1. Guel, M.D. *The SANS Policy Primer.* Bethesda, MD: The SANS Institute, 2007.

2. Harman, L.B. *Ethical Challenges in the Management of Health Information,* Second Edition. Gaithersburg, MD: Aspen Publishers, Inc., 2006.

3. World Wide Web Consortium (W3C) Web standards.

4. 45 *CFR* Parts 160 and 16, Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule. *Federal Register* 75:134 (July 14, 2010).

5. 45 *CFR* Part 70, Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule, July 28, 2010.

CHAPTER 1

Sample Policy

POLICY 1

ACCEPTING RESTRICTIONS REQUESTED BY INDIVIDUALS

Department:	**Policy Number:**	
Section:	**Effective Date:**	**Page:**
Title: Accepting restrictions requested by individuals	☑ **Non-Clinical** ○ **Clinical**	
Approved By:	**Review Date:** **Revision Date:**	

Scope

In compliance with the Health Information Portability and Accountability (HIPAA) privacy rule, individuals have the right to request, in writing, restrictions on the uses and disclosures of their protected health information (PHI) retained by this organization in its designated record set. Further, under the **45 CFR Parts 160 and 164 Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule, July 14, 2010 (p. 40899) requires organizations to accept restrictions on disclosing health information about services performed to payers when a patient pays cash for the services.**

Policy statements

Because such restrictions carry significant risk to the individual and to the organization, the organization will review each request for restriction and assess its ability to manage the restriction in all aspects of information management. The organization may accept restrictions:

- once the individual acknowledges all of the risks, as well as the obligations of the organization to use or disclose the PHI in the event of an emergency treatment requirement
- once the organization has documented the administrative, physical, and technical capability of complying with the restriction
- and if the individual's attending physician or other licensed healthcare professional finds that the organization's ability to provide quality healthcare services will not be compromised

A copy of all requests for restrictions and their resultant actions will be filed in the individual's medical record as well as with the information privacy official who will review requests for consistency with this policy. The original will be given to the individual making the request. Any restrictions accepted will not apply if the restricted information is needed to provide emergency treatment. Members of the medical staff or employees who accept restrictions by any other means than set forth in this policy or who willfully deny a restriction that can be accepted will be disciplined to the fullest extent of their privileges or employment contract.

Effective date: August 1, 2010

See also: Policy on assigning an alias for endangered individuals

HCPro

Order your copy today!

Please fill in the title, price, order code and quantity, and add applicable shipping and tax. For price and order code, please visit *www.hcmarketplace.com*. If you received a special offer or discount source code, please enter it below.

Title	Price	Order Code	Quantity	Total
				$

Your order is fully covered by a 30-day, money-back guarantee.

Shipping* (see information below)	$
Sales Tax** (see information below)	$
Grand Total	$

➲ **Enter your special Source Code here:**

Name

Title

Organization

Street Address

City State ZIP

Telephone Fax

E-mail Address

***Shipping Information**
Please include applicable shipping.
For books under $100, add $10. For books over $100, add $18. For shipping to AK, HI, or PR, add $21.95.

****Tax Information**
Please include applicable sales tax.
States that tax products and shipping and handling: CA, CO, CT, FL, GA, IL, IN, KY, LA, MA, MD, ME, MI, MN, MO, NC, NJ, NM, NY, OH, OK, PA, RI, SC, TN, TX, VA, VT, WA, WI, WV.

State that taxes products only: AZ.

BILLING OPTIONS:

□ Bill me □ Check enclosed (payable to HCPro, Inc.) □ Bill my facility with PO # ____________

□ Bill my (✓ one): □ VISA □ MasterCard □ AmEx □ Discover

Signature Account No. Exp. Date

(Required for authorization) (Your credit card bill will reflect a charge from HCPro, Inc.)

Order online at *www.hcmarketplace.com*

Or if you prefer:

MAIL THE COMPLETED ORDER FORM TO: HCPro, Inc. P.O. Box 1168, Marblehead, MA 01945

CALL OUR CUSTOMER SERVICE DEPARTMENT AT: 800/650-6787

FAX THE COMPLETED ORDER FORM TO: 800/639-8511

E-MAIL: *customerservice@hcpro.com*

Code: EBKSMPL