

Important news
about insurance and
risk management for
hospices and home
health care agencies.

The Importance of Credentialing

Betty Norman, BSN MBA CPHRM



Credentialing and privileging are processes of formal recognition and attestation that a physician or advanced registered nurse practitioner (ARNP) is both qualified and competent. Credentialing verifies that the individual meets standards set by the organization. This can be determined by reviewing such items as a completed application, as well as the individual's license, experience, certification, education, training, malpractice history and any adverse clinical occurrences. Consideration should also be given to an assessment of their clinical judgment and character through the use of interviews, professional references and referrals.

Privileging defines a physician's scope of practice and the clinical services he or she may provide within your organization. Privileging is based on demonstrated competence for specific procedures and activities and is a data-driven process. Physician and ARNP credentialing is usually done at initial appointment and at regular intervals (usually two years) or what is called reappointment. This process is a common step taken in any health-related organization.

Keep in mind that:

1. Credentialing is primarily performed to protect patients. It is one of the most effective controls in medicine today and probably ranks right up there with residency training as a key to quality.
2. Credentialing is also performed to protect the organization in case a patient is (or believes he/she has been) injured. Corporate negligence cases often allege that the organization did not perform the credentialing function well. Good credentialing practices allow your organization to easily demonstrate that you dotted all of the i's and crossed all of the t's. There's no question that if you do your job well, it becomes more difficult for a plaintiff attorney to demonstrate negligent credentialing.
3. Evaluating one's peers is one of the oldest principles executed among medical staffs. It dates back to the American College of Surgeons in the early part of the 20th century. Who better than other practitioners to determine whether a physician is qualified?

INSIDE THIS ISSUE

Integrating Quality and Performance Improvement Organizationwide

Compliance Corner: HIPAA 2011

HiTech in the Hospice Environment

Who To Contact

INSERT

Patient Requesting Racial Preference for Caregiver: Unlawful Discrimination?



Follow HCCIS on Facebook

We welcome your comments and questions.

Bruce Williams
Update
P.O. Box 2726, York, PA 17405
1-800-233-1957
www.hccis.com



Protect your organization from a negligent credentialing claim.

Integrating Quality and Performance Improvement Organizationwide

Barbara Stover Gingerich RN MS FACHE CHCE



In 1972 Medicare legislation led to the Health Care Finance Administration (HCFA) mandating utilization reviews. These reviews were introduced within the hospital setting and were a first step in an ongoing focus on service, safety and quality care. Utilization Review, Quality Assurance, Continuous Quality Improvement, Total Quality Management, Improving Organizational Performance, Quality Improvement and Performance Improvement are initiatives that followed the 1972 legislation. The focus of each of these initiatives was on measuring and achieving quality, with the end results of improved patient safety, care quality and organizational excellence.

There are many resources available to organizations in pursuit of organizational excellence and performance improvement. Among these are the Agency for Health Care Research and Quality (<http://www.ahrq.gov/>), the National Association of Healthcare Quality (<http://www.nahq.org/>) and The National Committee for Quality Assurance (<http://www.ncqa.org/>).

• Agency for Healthcare Research and Quality (AHRQ)

The Agency for Health Care Research and Quality (AHRQ) was formerly known as the Agency for Health Care Policy and

Continued on page 3

The Importance of Credentialing

Continued from page 1

Physician Credentialing Time/Cost

You might say, "But we've never had a bad physician join our staff. Why do we have to go to all this trouble? It can be expensive and take a lot of time to do primary source verification." Or "We only use physicians who are known to our community, or who are affiliated with a local, accredited hospital."

One reason to go to "all this trouble" as stated above, is to protect the organization from a negligent credentialing claim. Another reason is to protect the organization from the bad publicity that arises when a problem physician is identified by the media.

Here are some actual headlines regarding problem physicians:

"Unlicensed Doctor Arrested"

"Doctor Arrested for Sexually Assaulting Patients"

"Doctor Arrested on Drug Charges"

"DEA Raid Leads to Doctor's Arrest"

Would you want to wake up in the morning and face a similar headline about

a physician or ARNP practicing in your organization? Something like this might show up in your community newspaper, or on your local TV station, or even go viral on the internet. Other organizations have experienced these issues as you can see from the headlines above.

We live in a mobile society and physicians and practitioners who encounter problems in one geographic region have been known to travel to other parts of the country to continue to practice. A thorough credentialing process and background review can sometimes bring to light past problems or issues.

What should a complete physician file include?

Physician files should be at least as complete as those files kept on the organization's employees, even if the physicians are contracted to provide service. Each file should include at a minimum:

- A completed application
- Current license*
- Current DEA registration*
- Evidence of relevant training, experience and competence*
- Professional experience and affiliations*
- Current Certificate of Insurance (COI)*

- Query of National Practitioner Data Bank for malpractice history*
- Applicable board certification information*
- Professional references and recommendations
- Criminal background check

* Evidence of continuing education

*Requires Primary Source Verification

So, why should we credential physicians?

The most obvious reason for physician credentialing is to assure that a physician applying for privileges at your organization has the appropriate education and experience to work with your given patient population. A second reason is to assure that the information provided on the application is complete and truthful. This should be as true for physicians and ARNPs who are employed or contracted by your organization as it would be for any employee. But the most important reason for credentialing of professional healthcare providers is to assure quality patient care. If done correctly and comprehensively, credentialing ensures that patients receive quality medical care from qualified practitioners. ❤️

Research (AHCPR). The Healthcare Research and Quality Act of 1999 supported the establishment of this agency, which is one of the Department of Health and Human Services' (DHHS) 12 agencies. The overall mission of this agency is to improve all Americans' health care in the areas of quality, safety, efficiency and effectiveness. Success is measured by improved quality of life and patient outcomes, lives saved and value for dollars spent. Focusing on research and training, AHRQ gathers, evaluates and builds a knowledge foundation on which to establish policy and practice standards.

• **The National Association for Health Care Quality (NAHQ)**

This association began in California, as early as 1976, with a focus on bringing together quality professionals on a national and international level. Over ten thousand professionals are active within this association, which focuses on education and networking. The association provides resources and products geared to support and enhance the work of quality professionals.

• **National Committee for Quality Assurance (NCQA)**

In 1990, this private 501(c) (3) not-for-profit organization was formed, with a focus on improving health care quality. NCQA seeks to bring attention to and elevate the priority of health care quality on the national agenda. Its simple formula for improvement is (1) Measure, (2) Analyze, (3) Improve, and (4) Repeat, which is similar to many other commonly adopted quality/performance improvement formulas. All the formulas strive to operationalize and maximize quality/performance improvement initiatives and results throughout the organization.

Assimilating Quality/Performance Improvement Actions

In the development stage of a Quality/Performance Improvement Plan, a SWOT analysis, that includes scrutiny of Strengths, Weaknesses, Opportunities, and Threats (SWOT) should be conducted. Suggested target areas to explore in the SWOT analysis include: financial status, mission, values, ethics, organizational culture, programs, personnel, public image, service area, organizational maturity, clinical expertise/competency, surrounding community, competition, service area demographics, labor relations, patient population, reimbursement streams and

accreditation and regulatory bodies.

(Source: Gingerich. *Home Health Redesign*)

With the SWOT analysis in hand, a plan can be developed via the use of an organization wide steering committee, with a focus on a written, multidimensional plan that encompasses staff, contractors, volunteers, board, functions and services. A collaborative approach will engage participants early in the plan development and assist during the staff education and implementation stages, as well as the ongoing performance evaluation and action stages.

Plan Models

There is no correct plan/design model, but here are some that are commonly employed:

PDCA

Plan the improvement.
Do the improvement.
Check the results.
Act to hold the gain.

FOCUS PDCA

Find a process/procedure to improve.
Organize a team.
Clarify current knowledge.
Understand causes of variation.
Select the process improvement.
Plan the improvement.
Do the improvement.
Check the results.
Act to hold the gain.

FADE

Focus on the problem (or opportunity).
Analyze the problem (or opportunity).
Develop solutions and/or improvements.
Execute solutions/improvements and monitor their effectiveness.

Indicators and Data Collection

Indicator Selection - Organizations are encouraged to select several diverse indicators to measure and evaluate. In the past, high risk and high volume services, as well as outcome and process indicators, made up the indicator selection list. In addition, organizations usually include sentinel events, risk management events and unexpected outcomes, among others, in their indicator selection, data collection and monitoring activities.

Data Collection - Data collection activities should result in gathering meaningful and useful information that can be aggregated and trended for interpretation. Data will prove to be more valuable if there is ability to internally and/or externally benchmark findings. Organizations collect data from various formats and locations, such as

surveys, utilization reviews, record audits (administrative, clinical), work tools, timesheets, travel logs, clinical outcome tools, emergency management drills and organization-specific data collection tools. One commonly used data collection tool is the fish bone diagram (known as a cause and effect diagram). The fish bone diagram allows for group participation and provides a visual of information gathered.

Once data is gathered, statistical tools can be used to evaluate the extent of the 'potential problem/issue.' Aggregating data and using either a histogram or bar graph to display the data, allows the organization to compare performance and diagnose problems. Other useful graphic statistical tools that are easy to use are the pie chart and the Pareto chart.

Comparing findings to established thresholds, evidenced based practice standards, regional, local and national databases, such as the home health and hospice outcome measurement standards, allows for internal and external benchmarking over time and comparison between teams or branches of the organization.

Taking Actions

Data findings and results are really only one step in the quality process. It is what the organization does with its findings that results in performance improvement. Findings must be evaluated for strategies to improve outcomes. This process often requires a team approach, with a team made up of those closest to the concern, as well as those remote from the concern. This gives the group the benefit of a combined perspective, and objectivity can emerge in seeking, identifying and choosing the solution(s). It is also important that findings requiring attention do not get lost in the day-to-day operational issues. Developing a comprehensive action plan that becomes integral to the performance improvement plan makes it is less likely that concerns will be overlooked.

A performance improvement/action plan has several key headings. These include the basics of the action plan – the who, what, when, where and how. For example the action plan should include date, the findings, solution(s) selected for implementation, individual or group assigned responsibility for the implementation, date by which this action is to be completed, reevaluation date(s), and ongoing remonitoring dates to assure that any achieved improvement is maintained.

Integrating Quality and Performance Improvement Organizationwide, *continued from page 3*

A sample action plan format is provided below.

Date	Findings	Solution(s) to Implement	Assigned Responsibility	Action Completion Date(s)	Re-evaluation Date(s)	Findings	Ongoing Monitoring Dates/Actions

In some cases organizations will need to develop an action plan sheet for each finding and they should be retained, perhaps in a three-ring binder, and kept with the Quality/Performance Plan. Once the action plans are developed, it might be necessary to assign a priority to the implementation; however, any action required that directly affects patient care, safety, quality and outcomes should be immediately addressed without delay. In some cases several solutions might be chosen for a pilot study, so that a comparison of achieved results can occur and the solution demonstrating the best results can then be utilized across the organization.

It is not advisable to address findings without including ongoing follow-up evaluation and monitoring. Otherwise, the problem may resurface through lack of attention to ongoing monitoring and follow-up. Diligence and attention to details are keys to a successful action plan. Another important step in action planning is to report findings and progress to the board and staff and to provide education relative to any revised forms, policies, processes and procedures.

Summary: Simple Steps

Leadership and the governing board have the ultimate responsibility for establishing organizational objectives and evaluating performance. The overall task of developing a quality/performance improvement plan is only the first step in assuring that quality standards and processes are instituted and adhered to throughout the organization. It is important that there is ongoing oversight of measurements, findings, actions taken, evaluations and reassessment of effectiveness of the overall plan. It is through this ongoing analysis, action taking and evaluation that organizational excellence can be achieved and maintained.

There are many simple steps that must be taken in order to achieve the overall organizational excellence and improved performance results intended by any

performance improvement plan. Each step is necessary to achieve the desired outcomes and meet the performance improvement expectations required.

In summary, the steps include:

- Assign the responsibility - team, individual
 - Complete an organizational analysis
 - Choose a design model, for example
 - FADE, PDCA, FOCUSPDCA
 - Establish indicators
 - Sentinel events, rate based, outcomes, process
 - Verify and establish practice guidelines, including
 - Competency
 - Practice standards
 - Benchmarking
 - Home health/hospice compare
 - Customer satisfaction levels
 - Collect and monitor indicators, including
 - Utilization rates
 - Variance/variable measurements
 - Causative analysis: common, special, unknown or assignable
 - Select and use statistical measurement tools such as
 - Benchmark
 - Scatter diagram
 - Line graph
 - Bar graph
 - Histogram
 - Pie chart
 - Document, evaluate, communicate findings to staff, board as required
 - Action plan development, implementation, evaluation and remonitoring
 - Revise actions taken, as needed
 - Continue ongoing monitoring
 - Conduct an annual evaluation of the total performance improvement activities and plan
 - Revise and update total performance improvement plan as needed
- (Gingerich, Quality/Performance Improvement Plan, Advantage Consultants, Inc)*

It is only possible to maintain improvement, by vigilance, repetition, remonitoring and reevaluating. It is critical that board and staff understand findings and actions taken throughout the process and that external regulators are notified of findings as required. In seeking solutions to problems, creativity and receptivity are important, as well as a willingness to try more than one solution, allowing for comparing achieved outcomes and choosing the solutions achieving the best results. ♥

References/Resources

Gingerich, BS. *Home Health Redesign: A Proactive Approach to Managed Care*. Aspen Publications: Gaithersburg MD.

Gingerich, BS. *Quality/Performance Improvement Plan*. Advantage Health Care Management Resources Press: York PA.

Institute for Health Improvement. *Science of Improvement: How to Improve*. Retrieved on July 23, 2011 from <http://www.ihl.org/knowledge/Pages/HowtoImprove/ScienceofImprovementHowtoImprove.aspx>

National Association for Health Care Quality. *About NAHQ*. Retrieved on July 23, 2011 from www.nahq.org

National Committee for Quality Assurance. *About NCQA*. Retrieved on July24, 2011 from www.ncqa.org

US Department of Health and Human Services. Agency for Healthcare Research and Quality. *Frequently Asked Questions*. Retrieved on July 26, 2011 from www.ahrq.gov

US Department of Health and Human Services. Agency for Healthcare Research and Quality. *Measuring Health Care Quality*. Retrieved on July 26, 2011 from <http://www.ahrq.gov/qual/measurix.htm>

COMPLIANCE CORNER:

HIPAA 2011

Barbara Stover Gingerich RN MS FACHE CHCE
President, Advantage Consultants, Inc

BACKGROUND

Health Insurance Portability and Accountability Act (HIPAA)

The Privacy Rule enacted in 2003 became effective in 2005, with 2009 targeted as the effective date of its security components. The Privacy Rule was enacted to expand federal protection for personal health information (PHI) held by covered entities and to also define patients' rights with respect to that information. The rule does permit the disclosure of personal health information needed for patient care and other important purposes. However, sharing information without permission and demonstrated need can result in civil and criminal penalties. The original 1996 HIPAA focus had four elements, i.e., (1) educating consumers regarding costs for services with the Explanation Of Medicare Benefits (EOMB), (2) expanding coverage of HIPAA requirements beyond Medicare and Medicaid to private insurers, (3) enhancing enforcement activities with increased funding and (4) expanding penalties.

Another HIPAA focus is fraud and abuse, specifically in the areas of kickbacks and billing. The four most prevalent identified billing abuses are upcoding bills, billing for known noncovered services, providing and billing for medically unnecessary services and/or billing for care and services never provided.

Recent Enforcement

The Department of Health and Human Services delegated to the Office for Civil Rights (OCR) the authority to administer and enforce the HIPAA Security Rule. Penalties can include felony conviction, civil monetary penalties (up to three times \$11,000 per mistake), and exclusion from Medicare, Medicaid and payor program participation. This exclusion can range in time from one year to permanent exclusion. As HIPAA enforcement moves forward, there have been ongoing revisions to penalties and while penalties had not been significant to date, recently two enforcement penalties were issued that give health care organizations a renewed reason to look at

their operations, education and protocols.

In one recent case, the Office for Civil Rights (OCR) issued its final determination that Cignet Health of Prince George's County, MD violated the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as the Health Information Technology for Economic and Clinical Health (HITECH) Act. As a result, Cignet was assessed a civil money penalty of \$4.3 million.

The Cignet case was shortly followed by another case, which ended with the Department of Health and Human Services (HHS) and The General Hospital Corporation and Massachusetts General Physicians Organization, Inc., (Mass General) entering into a Resolution Agreement in which Mass General agreed to pay \$1,000,000 and to enter into a Corrective Action Plan (CAP) to implement policies and procedures, which would better safeguard the privacy of its patients. This came about as a result of ongoing potential violations of the HIPAA Privacy and Security Rules. In the Mass General case, the findings were based upon staff removing record information from the organization's location and losing it while in transit.

Corrective Action Plan (CAP) Elements

A comprehensive corrective action plan designates the individuals within the organization who are responsible for reporting specific actions, as well as a designated external monitoring group and a designated contact within Department of Health and Human Services' regional Office for Civil Rights. Any changes from the agreed upon designees must be communicated with and approved by HHS. The CAP also specifies policies and procedures that must be developed and put into place to address violations. These policies and procedures, as well as others that are developed by the organization relative to privacy and security, must be submitted to and approved by HHS. In addition the communication and



distribution of the new and/or revised policies and procedures are clearly specified in a CAP, as well as specific time frames for accomplishing the communication and distribution aspects of the CAP.

Education and training, including staff, board, volunteers and contractors, must be provided in order for policies and procedures to be considered fully implemented. Any additions, revisions or deletions to the policies and procedures requested by HHS must be made within a specified time frame (usually 30 days), with a full implementation time frame often specified at 60 days. Minimal content, along with training specifics, is also included in a Resolution Agreement's Corrective Action Plan. The designated Monitor (approved by HHS) will submit a written Monitor plan to the organization and HHS. This plan must meet with the approval of HHS. Monitor responsibilities include conducting assessments of implementation and compliance with the Corrective Action Plan, investigating any reportable events, interviewing workforce members, evaluating policies and procedures compliance and adherence, conducting onsite record audits, making unannounced inspections, including inspection of computer records, computers, laptops and flash drives, and training records and submitting written reports of findings at least twice per year. At a minimum, an annual review of policies and procedures is required.

Continued on page 6

HIPAA 2011

Continued from page 5

Health Privacy Complaint Process

Anyone can file a complaint, and organizations cannot retaliate against the complainant. A complaint can be in writing, sent by paper, electronically, or faxed. The Health Information Privacy Complaint Form Package is readily available online for download. Organizations can also request a copy via the OCR regional office.

Organizations should obtain a complaint package and review the contents. This package is available in numerous languages, including Chinese, Korean, Polish, Russian, Spanish, Tagalog and Vietnamese. Including this package in staff educational in-services, focused on increasing staff awareness about the privacy and security regulations and their role in assuring compliance, is a good strategy to utilize to increase staff awareness and understanding. Although there is a 180-day time limit for filing a complaint calculated from the date of the action or omission, if the complainant can demonstrate a good reason/cause for not filing the complaint in a timely basis, this time frame can be extended by the OCR. The regional OCR and office manager is where the complaint is initially addressed.

OCR has the authority to determine what constitutes a violation, and whether it is one violation or multiple violations according to the circumstances of the breach, numbers of individuals involved, the time frame over which the breaches occurred, and time frame from the occurrence to taking action.

Decreasing Exposure and Risk

A good approach is to develop policies and procedures that adhere to the privacy and security regulations and that meet regulatory intent. Self-reporting, along with actions taken, can result in lowered penalties and organizational impacts of enforcement by the HHS/OCR. Not taking action regarding a potential privacy or security breach can lead to increased organizational impacts resulting from the violation. By taking prompt appropriate action, it is less likely that HHS/OCR investigation will result in a finding of willful neglect. Willful neglect penalties can range from of \$10,000 per violation, with corrective action taken within 30 days of the violation, to a maximum of \$50,000 per violation. The higher amount is more

likely to be assessed if the organization has not notified the individuals affected by the security/privacy breach. Leaving an identified violation uncorrected could lead to more than \$1 million per violation in penalty assessments.

Another area of exposure is contracting with other providers and hiring staff. It is important that organizations are aware of any excluded providers and that organizations do not participate with any excluded providers. Organizations that participate with an excluded provider are penalized \$10,000 per penalty. Organizations must communicate that there is a zero tolerance to unethical behavior and their staff must routinely access the DHHS's data bank of sanctioned health care organizations and providers. The Division of Practitioner Data Banks (DPDB), which is responsible for National Practitioner Data Bank (NPDB) and Healthcare Integrity and Protection Data Bank (HIPDB), offers educational outreach to assist organizations in remaining compliant and knowledgeable of resources to support health care integrity and practices.

HIPAA 4010A1 to HIPAA 5010

There are differences between the HIPAA 4010A1 and HIPAA 5010, in that the HIPAA 5010 is intended to better support new-use cases brought forward by the industry, provide usage clarification, increase consistency across transactions, support National Provider Identifier (NPI) regulation, and delete data content when it is no longer needed. This upgrade became necessary due to some unanticipated issues and requirements that could be better met, as upcoming mandatory ICD-10-CM and ICD-10-PCS code sets are implemented.

In conjunction with the upgrade to HIPAA 5010, the HIPAA Eligibility Transaction System (HETS) allows the release of eligibility data to Medicare providers, suppliers, or their authorized billing agents for the purpose(s) of preparing an accurate Medicare claim, determining beneficiary liability or determining eligibility for specific services. Such information may not be disclosed to anyone other than the provider, supplier, or beneficiary for whom a claim is filed. At this time physicians, hospitals, payers, clearinghouses, pharmacies and dentists are required to upgrade to HIPAA 5010 standards, but can use a clearinghouse to assist them with complying with the rules. At this time software vendors, while not included in the list of covered entities, will need to

upgrade their products to support their customer needs.

It is important to remain knowledgeable about ongoing HIPAA revisions and the pilot testing and implementation of the 5010 as it is put into place for the current listing of providers. It is anticipated that in the future HIPAA 5010 will be extended to all Medicare provider groups. The new 5010 version supports and requires the use of ICD-10 codes, and the Office of e-Health Standards and Services (OESS) within CMS is responsible for checking compliance with HIPAA 5010.

Summary

Resources are available to assist organizations in their understanding and application of required privacy and security actions. For example, A Summary of the HIPAA Privacy Rule, a 25-page document, is available for access and download at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>. This document is a good reference to download and retain in the administrative files as a current and future resource. It is also important to determine if the organization's state has additional privacy and security requirements that are more stringent or more encompassing than the Federal regulations. If that is the case, organizations must adhere to the additional state requirements in order to fully meet privacy and security requirements and regulations. ♥

References/Resources:

Electronic Data Interchange System Access and Privacy. Retrieved on July 24, 2011 from http://www.cms.gov/ElectronicBillingEDITrans/02_SystemAccess.asp#TopOfPage

HIPAA News. Org. *Protecting the Privacy of Personal Health Information.* Retrieved on July 24, 2011 from <http://www.hipaanews.org/>

How to File a Complaint. Retrieved on August 3, 2011 from <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>

OCR Summary of the HIPAA Privacy Rule. Retrieved on July 22, 2011 from <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>

Regulations. HIPAA Information Privacy. Retrieved on July 26, 2011 from <http://www.hhs.gov/policies/index.html>

The Data Bank. National Practitioner Health Care Integrity and Protection. Retrieved on August 3, 2011 from <http://www.npdb-hipdb.hrsa.gov/>

US Department of Health and Human Services. *Health Information Privacy. News Archive. February 2011.* Retrieved on July 23, 2011 from <http://www.hhs.gov/ocr/privacy/hipaa/news/index.html>

HiTech in the Hospice Environment

Laura Mosby, LCSW

Director of Organizational Integrity, Suncoast Hospice, Clearwater, Florida

Suncoast Hospice

Founded more than 30 years ago by volunteers, Suncoast Hospice is a community-based, not-for-profit agency committed to serving individuals and families. Its mission of care focuses on persons with chronic or serious illnesses and extends also to those acting as caregivers or working through grief and trauma. Suncoast Hospice is known for its innovative service delivery, social change advocacy, technological development and other end-of-life initiatives.

A Little HiTech History

In 2009 the Health Information Technology for Economic and Clinical Health (HiTech) Act became a reality for Hospices. This was an expansion of the previous Health Insurance Portability and Accountability Act (HIPAA) of 2003. This new HiTech Act required that all Hospices and their Business Associates (BAs) become more aware, active, and accountable in protecting the security and privacy of personal health information. This regulation clearly defines breaches of unsecured protected health information and spells out the responsibility for notification in the event of a breach. Essentially, the act details the what, who, how, and when of notification requirements. Additionally, this act levies significant sanctions for breach violations depending on the intentionality and severity of the breach. Complete detailed information regarding HIPAA and HiTech can be found on the Health and Human Services, Office of Civil Rights website (www.hhs.gov).

Definitions

A Breach of unsecured protected health information is defined as the acquisition, access, use, or disclosure of protected health information to unauthorized individuals which compromises the security and privacy of the protected health information.

A Breach excludes:

A. Any unintentional acquisition, access, or use of protected health information by a member of the

workforce or person acting under the authority of the Organization or its BAs where such actions were made in good faith, within their scope of authority, and does not result in further disclosure.

B. Any inadvertent disclosure by a person who is authorized by the Organization or BA in providing information to another person who is authorized to access information at the same Organization, BA or other organized health care arrangement with whom the Organization participates, in which the information received is not further used or disclosed.

C. A disclosure to an unauthorized individual, where the Organization or BA has a good faith belief that the unauthorized person would not reasonably be able to retain the information

committee to review current practice and enhance our programs and processes as needed. The committee focused on several areas:

- Process for breach assessment, notification, and reporting
- Securing electronic protected health information: encryption
- Relationships and agreements with Business Associates
- Staff education
- Policies and procedures

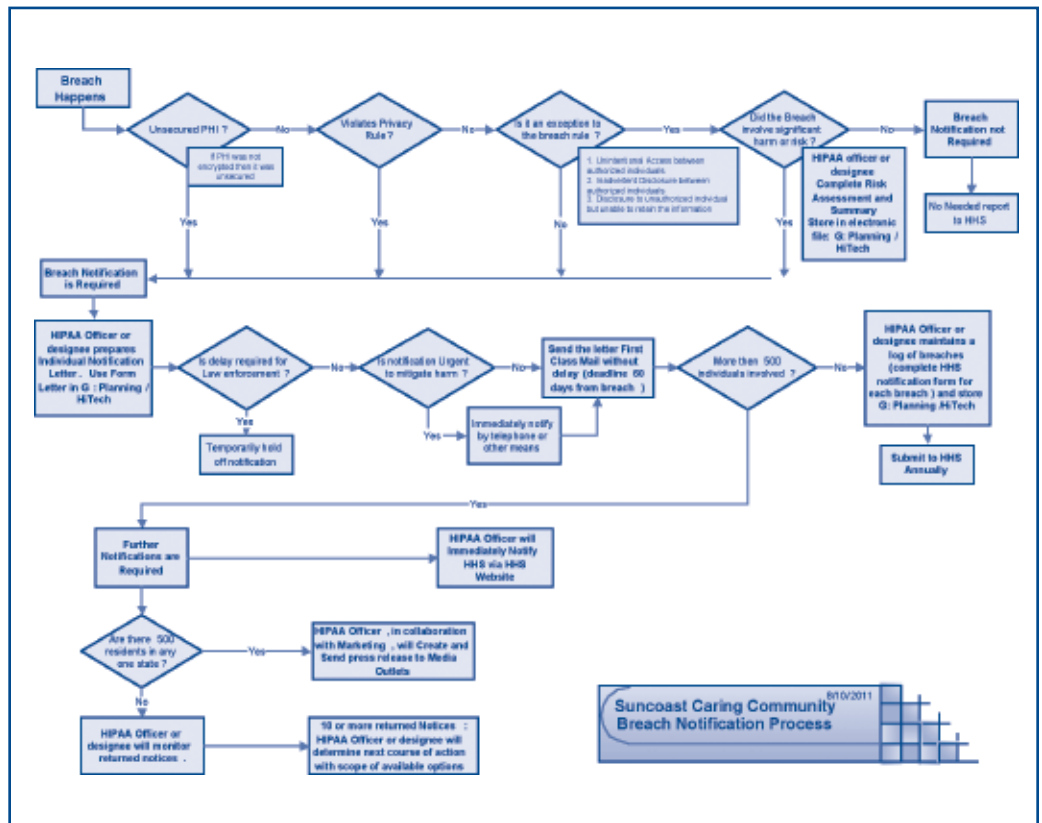
Process for Breach Assessment, Notification and Reporting

The new HiTech regulations require that assessments, notifications, logs and reporting be effectively managed. At Suncoast, we clarified additional roles and responsibilities for the HIPAA Officer and developed the following process to clarify decision-making regarding notifications and reporting. Policies and procedures were written to reflect these new processes and roles.

Continued on page 8

Implementing HiTech at Suncoast Hospice

In 2009, with HiTech looming on the forefront, Suncoast Hospice established a



HiTech in the Hospice Environment

Continued from page 7

Additional Preparation

Suncoast Hospice worked with all of our Business Associates to ensure that new agreements were in place and that each BA had the necessary knowledge and resources to comply with the new HiTech expectations. We provided additional literature and consultation when necessary. There are a variety of affordable educational resources on the market to assist BAs' who might otherwise be unfamiliar with the HIPAA and HiTech.

Staff education was enhanced. All new employees attend orientation and presentations relating to HIPAA. This session was enhanced to now include the required HiTech training. Additionally, annual updates and refreshers are required for all employees. The leadership team at Suncoast Hospice participates in several in-service presentations regarding HIPAA and HiTech throughout the year. These trainings highlight the concept that protecting the health information of our

patients and clients is a shared responsibility for all in the organization. Lastly, our Health Information Department offers several awareness campaigns throughout the year. Helping to maintain staff awareness is key to successfully preventing breaches.

Living with HiTech

With ever advancing technology and the need to effectively communicate patient information in a seamless yet safe manner, it becomes more and more important that the culture of all health care organizations evolve to match a new level of sophistication in the management of patient information. Organizations must obtain new required expertise, revise processes and practices, and embrace the responsibility of protecting patient health information in a new way. Now, two years into implementing a program to support the HiTech regulations, we at Suncoast find that our overall awareness and sense of accountability has risen and continues to rise to meet the challenge. ❤️

Who to Contact

Hospice and Community Care Insurance Services
P.O. Box 2726, York, PA 17405
1-800-233-1957 • Fax: 717-747-7021

hccis.com

Members who insure directly with us (not through another agent or broker), please request Certificates of Insurance, submit claims, make policy changes, or ask questions about your policies, by contacting your Customer Service Representative
Sheila Simmons, Ext. 7595 who services all states.

Insurance Brokers, please contact the Underwriter responsible for your state.

Mike Hetrick, Ext. 7535
West: AK, AZ, CA, CO, HI, ID, MT, ND, NE, NM, NV, OR, SD, UT, WA, WY

Greg Lindstrom, Ext. 7561
Southeast: FL, GA, NC, SC

Michelle Bethas, Ext. 7553
Northeast: CT, DC, DE, MA, ME, NH, NJ, NY, PA, RI, VT

Sheri Eckenrode, Ext. 7588
South Central: AL, AR, KS, LA, MS, OK, TX

Sarah Vail, Ext. 7541
Midwest: IA, IL, IN, KY, MD, MI, MN, MO, OH, TN, VA, WI, WV

Administered by Glatfelter Underwriting Services, Inc.
and/or a Glatfelter Insurance Services in CA, MN, NY, TX, and UT
and Glatfelter Brokerage Services in NY

To print additional
copies of the newsletter,
visit our web site at
www.hccis.com

P.O. Box 2726, York, PA 17405

Hospice and Community Care Insurance Services
A Division of Glatfelter Insurance Group

Update

PRSRST STD.
U.S. POSTAGE
PAID
YORK PA
PERMIT NO. 631