

Rush Health Systems

Rush Foundation Hospital – H. C. Watkins Hospital – Laird Hospital – Scott Regional Hospital – Specialty Hospital of Meridian – Stennis Hospital – Choctaw General Hospital - MFI - Rush Medical Group

GENERAL ORIENTATION TO COMPLIANCE

WELCOME to Rush Health Systems! Thank you for becoming a member of our healthcare team. Below are some basics in compliance for the world of healthcare. Your contact for compliance is

***Cathy Robinson, CHC
Chief Compliance Officer
1800 12th Street
6th Floor, Professional Office Building
Meridian, MS 39301
601-703-9493
cathy.robinson@rushhealth.com
Rush External Hotline # 1-800-826-6762***

Please do not hesitate to call me at any time for any questions or concerns regarding compliance.

WHAT IS COMPLIANCE?

COMPLIANCE is DOING THE RIGHT THING, each time....every time. I read a definition of “Integrity” once which said “when you do the right thing even though no one is watching”. Henry Longfellow said “it takes less time to do a thing right than to explain why you did it wrong.” Janis Joplin said “Don’t compromise yourself – it’s all you’ve got”. An anonymous quote said “stand up for what is right, even if you are standing alone!” These quotes bring several words to mind: integrity, ethics, character, principles – they all play a part in “compliance”. Rush works really hard to maintain a culture of COMPLIANCE.

We spend a lot of time and effort on EDUCATION. The *Code of Conduct* and the quarterly publication “*Compliance Communicator*” are two means we use for education. From time to time, we have very specific targeted education on various topics. We also spend a lot of time on AUDITING AND MONITORING. We do our very best to be sure we are in compliance. BUT...IT TAKES YOU being a part of compliance for our efforts to be most successful.

CODE OF CONDUCT:

You have received a copy of the Code of Conduct. This sets forth the foundation for compliance at Rush Health Systems and its affiliated entities. As a refresher for this Orientation, the contents include:

- ◆ Introduction to the Code of Conduct
- ◆ Our Mission, Vision, and “House Rules”/Values
- ◆ Quality of Care
- ◆ Statement of Ethics
- ◆ Non-Discrimination
- ◆ Compliance with Laws and Regulations
- ◆ Conflicts of Interest
- ◆ Gifts and Gratuities
- ◆ Referral and Kickbacks
- ◆ Protection of Property
- ◆ Proper Consideration of Human Resources
- ◆ Harassment and Workplace Violence
- ◆ No Solicitation/No Distribution
- ◆ Communication

- ◆ Billing and Coding
- ◆ Sanctioned Individuals
- ◆ Addressing Issues and Concerns
- ◆ Open Door Policy
- ◆ Non-Retaliation
- ◆ Other Concerns
- ◆ Certification of Receipt and Understanding

We are going to talk a little further about some of these topics.

OPEN DOOR POLICY – ASK QUESTIONS IF UNSURE – BRING CONCERNS TO THE ATTENTION OF YOUR MANAGER OR THE COMPLIANCE OFFICER:

Individuals have the ability to report real or perceived fraud and abuse to the Government (whistleblower). The Rush Culture encourages individuals to ask questions and to bring concerns to us using the Chain of Command. Anyone can bring any concern to the Compliance Officer at any time. This is our Open Door Policy. An individual can call or see the Compliance Office at any time or use our internal or our external Hotline to report a concern anonymously. We consider ourselves to have a very robust Compliance Program, and we investigate and followup any concerns brought forward. We also have a Non-Retaliation Policy to further encourage individuals to discuss their concerns with us, which allows us to determine if there is in fact an issue and correct that issue if there is one.

We encourage, actually require, our coders to query the physician on any questions they may have when coding the diagnoses and procedures. We hope that you will certainly support this, as this is for your ultimate benefit.

HANDLING OF ANONYMOUS COMPLIANCE OR HUMAN RESOURCE RELATED QUESTIONS, COMMENTS OR CONCERNS:

Rush Health Systems has two methods for communicating a comment or concern anonymously.

1. **External Hotline Service:** 1-800-826-6762. When you call this number, they will type your comments, assign your call an identification or reference number, and provide you with that reference number and a callback date. In the meantime, your comment or concern is emailed by the Hotline Service to me, Cathy Robinson, Compliance Officer to investigate. I will contact the Hotline Service prior to the callback date they provided to you with a response. When you callback, they read my response to you. Occasionally, I may ask for additional details so that I may be able to provide a more thorough investigation, and I hope that you will provide that.
2. **Internal Rushnet “Break with the Boss”:** This is similar to the external Hotline Service in that you are not required to provide your identity and it cannot be traced back to you. With this method, the only way we have of responding back to you on your comment or concern is via the *Rush Remedy* newsletter or by having the department manager voice a response department-wide, if we are aware of the department involved. There are times when it is not appropriate to print a response in the *Rush Remedy*.

INFORMATION REGARDING YOUR CONCERN: While I encourage you to feel comfortable to talk with me personally at any time and make every effort to assure you of privacy, I understand that there may be times when you still feel more comfortable with anonymity. In those situations, let me ask you to please provide enough information that will allow me to properly investigate your concern or comment. Rush Health Systems is very large with many facilities in various locations. A comment such as “employees are wasting the hospital’s money by taking too many breaks” is something we certainly want to know about, but we have five hospitals and many clinics, each of which have multiple departments. There isn’t much way of investigating this adequately. So, please provide enough details that I will be able to properly investigate your concern.

INVESTIGATION AND RESPONSE TO ANONYMOUS QUESTIONS, CONCERNS OR COMPLAINTS: As you can see from the above information, (1) we want you to voice any questions, concerns or complaints you have. While we encourage you to talk with the Compliance Officer directly, we respect your desire for anonymity. With this in mind, (2) we take all questions, concerns and complaints very seriously, and (3) investigate them to the fullest extent possible. We need as much information as you can provide to do this properly. (4) We want to provide you a response. Sometimes with anonymity, this is difficult. There is sometimes a fine line between trying to properly

investigate the issue and provide you a response while at the same time keeping your anonymity. We really do try our very best. I welcome your input and your comments as to how this works for you.

NON-RETALIATION:

We have a non-retaliation policy. If you ever feel you have been retaliated against for having voiced a concern or question, please notify me immediately. Let's look first, however, at what isn't "retaliation". If you are in violation of company rules, guidelines, etc., you are subject to disciplinary action whether or not you coincidentally just voiced a question or concern. Voicing a concern doesn't negate disciplinary action as a result of inappropriate performance of your job or inappropriate conduct. Another example of what is not "retaliation" is when you voice a question or concern anonymously, and the only way to try to get the response to the person who anonymously voiced the question or concern is to discuss the issue in a departmental meeting. Also, it is possible that the identify of the person voicing a certain question or complaint may be obvious to your manager or co-workers. An investigation might very well involve talking to the person who made the complaint, unbeknown that this is the person who made the complaint. Retaliation for voicing a question, concern or complaint is still not acceptable. If you feel you have been retaliated against for voicing a question, concern or complaint, please notify the Compliance Office.

NON-DISCRIMINATION:

Rush has a strong "Non-Discrimination" policy, which is recapped under #3 in the Code of Conduct.

AMERICANS WITH DISABILITIES:

Rush recognizes the importance of making accommodations for those with disabilities.

Service animals are certainly permitted.

Rush will provide appropriate Auxiliary Aids and Services where such aids and services are necessary to ensure effective communication with Deaf Patients or Companions, as required by the ADA. Pursuant to 42 U.S.C. § 12182(a), Rush will also provide Patients and Companions who are deaf or hard-of-hearing with the full and equal enjoyment of the services, privileges, facilities, advantages, and accommodations of Rush as required by the ADA. Rush shall not deny its services, privileges, facilities, advantages, and accommodations to anyone based on the fact that the person is Deaf or is associated with someone known to be Deaf, as required by the ADA. At Rush Foundation Hospital, contact the Nursing "House" Supervisor immediately for assistance with assessment of needs for the deaf and for interpretation assistance. At other Hospitals within Rush Health Systems, contact the Hospital Nursing Supervisor and in Clinics contact the Clinic Manager.

Rush has a contract with Language Line Services to provide prompt 24/7/365 access to interpretation services.

FEDERAL FALSE CLAIMS ACT:

Applies to "any person" who "knowingly presents or causes to be presented"

- ◆ A "false or fraudulent claim for payment" to the "United States Government"
- ◆ "Knowingly" includes acting in "reckless disregard of truth or falsity of the information"
- ◆ "No proof of specific intent to defraud is required"

The Centers for Medicare and Medicaid Services (CMS) defines "fraud" as the **intentional** deception or misrepresentation that an individual knows to be false (or does not believe to be true) and makes, knowing that the deception could result in an unauthorized benefit to himself or another person. CMS defines "abuse" as incidents or practices of providers that are inconsistent with sound medical practice and may result in unnecessary costs, improper payment, or the payment for services that either fail to meet professionally recognized standards of care or are medically unnecessary.

The Federal Government has enacted criminal and civil laws pertaining to the submission of false or fraudulent claims for payment or approval to the federal and state governments and to private payors. These false claims laws, which provide for criminal, civil, and administrative penalties, provide governmental authorities with broad

authority to investigate and prosecute potentially fraudulent activities, and also provide anti-retaliation provisions for individuals who make good faith reports of waste, fraud, and abuse.

The **False Claims Act** (31 U.S.C. §3729 *et seq.*) is a federal law that imposes liability on any person who:

- ❖ knowingly presents, or causes to be presented, a false or fraudulent claim, record or statement for payment or approval,
- ❖ conspires to defraud the government by getting a false or fraudulent claim allowed or paid,
- ❖ uses a false record or statement to avoid or decrease an obligation to pay the Government,
- ❖ and other fraudulent acts enumerated in the statute.

The term "**knowingly**" as defined in the False Claims Act ("FCA") includes a person who has actual knowledge of the information, acts in deliberate ignorance of the truth or falsity of the information, or acts in reckless disregard of the truth or falsity of the information. No proof of specific intent to defraud is required.

The term "**claim**" includes any request or demand for money or property if the United States Government provides any portion of the money requested or demanded.

Potential civil liability under the FCA currently includes penalties of between five thousand five hundred (\$5,500) and eleven thousand (\$11,000) per claim, treble (triple) damages, and the costs of any civil action brought to recovery such penalties or damages.

The **Attorney General of the United States** is required to diligently investigate violations of the FCA, and may bring a civil action against a person. Before filing suit the Attorney General may issue an investigative demand requiring production of documents and written answers and oral testimony.

The FCA also provides for **Actions by Private Persons** (*qui tam* lawsuits) who can bring a civil action in the name of the government for a violation of the Act. Generally, the action may not be brought more than six years after the violation, but in no event more than ten. When the action is filed it remains under seal for at least sixty days. The United States Government may choose to intervene in the lawsuit and assume primary responsibility for prosecuting, dismissing or settling the action. If the Government chooses not to intervene, the private party who initiated the lawsuit has the right to conduct the action.

In the event the government proceeds with the lawsuit, the *qui tam* plaintiff may receive fifteen to twenty-five per cent of the proceeds of the action or settlement. If the *qui tam* plaintiff proceeds with the action without the government, the plaintiff may receive twenty-five to thirty per cent of the recovery. In either case, the plaintiff may also receive an amount for reasonable expenses plus reasonable attorneys' fees and costs.

If the civil action is frivolous, clearly vexatious, or brought primarily for harassment, the plaintiff may have to pay the defendant its fees and costs. If the plaintiff planned or initiated the violation, the share of proceeds may be reduced and, if found guilty of a crime associated with the violation, no share will be awarded the plaintiff.

Whistleblower Protection. The False Claims Act also provides for protection for employees from retaliation. An employee who is discharged, demoted, suspended, threatened, harassed, or discriminated against in terms and conditions of employment because of lawful acts conducted in furtherance of an action under the FCA may bring an action in Federal District Court seeking reinstatement, two times the amount of back pay plus interest, and other enumerated costs, damages, and fees.

If you know of, suspect, or have a concern of a compliance nature, you have a duty to let your employer know promptly, so that the concern can be investigated and corrected, if a problem is found. If you do not feel your concern was investigated or addressed properly, you should elevate that concern to the next level of administration.....Remember you can ALWAYS contact the Compliance Officer at any point and at any time. As discussed above, you may report suspected violations to the Compliance Officer without fear of retaliation.

FRAUD AND ABUSE – BILLING AND CODING:

To repeat one of the examples above, all services you order require a signed, dated, and timed physician's order ALONG WITH documentation to support the medical necessity. The Government, including CMS, Office of Inspector General, Department of Justice, etc. has programs in place to detect fraud and abuse. There is "real" intention fraud and abuse, such as an individual renting space in a strip mall, hanging a sign in the empty window, having a post office box, and paying individuals \$5 or \$10 dollars to use their Medicare number to submit false claims to the Government for services never performed. Those are the people who get caught, fined, and put in jail. Then there are the honest, hard working individuals who forget to document the medical necessity for ordering certain tests or don't pay attention to Medicare's guidelines for approved indications for inserting certain medical devices, etc. who get fined, put under a five year Corporate Integrity Agreement because they "knew or

should have known” the rules. For the Government to find you in violation of the Federal False Claims Act, they do NOT have to prove you intended to defraud the Government. Below are some quick reminders:

- ◆ Order only the tests you truly need and whose results you are going to use for your patient.
 - ◆ Date, time and sign all orders. (That’s the CMS rule.)
 - ◆ Make sure your documentation in the record clearly supports the medical necessity (the reason) for ordering the test. (The government has hired companies like Connolly Healthcare to review records in comparison against its “rules” and for documentation of medical necessity. If not present, reimbursement will be recouped. A trend of these deficiencies or “errors” among physicians or hospitals can get you in a lot of trouble that the government calls “fraud and abuse”. (Remember, the intent to defraud does not have to be proven.)
 - ◆ Make sure you use the information from the test – acknowledging this in some way in the record. For example, if you order a chest x-ray on a patient and never look at it or acknowledge the results, the government considers that “abuse” (in other words, ordering and charging for services you never used – services you apparently didn’t need.)

MEDICARE RECOVERY AUDIT CONTRACTOR (RAC): Connolly Healthcare is the vendor for Region C (which includes Mississippi and Alabama) hired by CMS to review records for the sole purpose of finding some reason do deny the claim and recoup the reimbursement back to the Medicare Trust Fund. They compare the record and charges billed against various CMS billing rules and Conditions of Participation, and can then deny all or part of the charges. Hot targets for RAC reviews include, but are not limited to:

- ⤵ Coding or DRG errors
- ⤵ Lack of documented medical necessity
- ⤵ Lack of admission order for inpatients
- ⤵ Services provided in the wrong setting (acute inpatient versus outpatient with observation)

MEDICAID RECOVERY AUDIT CONTRACTOR (RAC): PRGX Global is the vendor for Mississippi Medicaid hired by the Mississippi Division of Medicaid to review records for the sole purpose of finding some reason do deny the claim and recoup the reimbursement back to the Medicaid.

HIPAA/HITECH:

Angie Sherrill is the Chief Information and Privacy Officer for Rush Health Systems.

- ◆ **HIPAA** is a federal law that protects the privacy of patients and all information about them. HIPAA gives patients the right to have their information kept private and secure. Remember: HIPAA is a federal law with penalties (even criminal ones) for violations that could be assessed on **you**.
- ◆ **HITECH** is a subset of the American Recovery and Reinvestment Act of 2009 (ARRA), which became federal law on February 17, 2009. The purpose of HITECH is to enhance and expand the HIPAA Privacy and Security rules, and not only makes privacy regulations more strict, but it gives more power to federal and state authorities to enforce privacy and security protections for patient data.
- ◆ **PHI** is protected health information. PHI is covered under HIPAA/HITECH, which established rules for when and how healthcare workers may use or release patients’ PHI.
 - ⤵ PHI includes any information that can be used to identify a patient, such as name, address, employer, relatives’ names, date of birth, telephone number, e-mail address, social security number, medical record and account numbers, photo, and other characteristics that could identify someone.
 - ⤵ PHI includes medical or health-related information if it can be tied to one specific patient, including; reasons the person is seeking healthcare, treatments and medications, test results, any observations about the patient, history, discharge information and billing information – basically anything about the patient.
 - ⤵ The law only permits healthcare workers to use and share PHI to perform their job for three reasons without the patient’s permission:
 - Treatment
 - Payment
 - Healthcare Operations

- ⚡ Healthcare workers can **ONLY** access a patient's PHI in the course of directly performing his/her specific job duties. Just because you work at the healthcare facility does **NOT** mean you can access a patient's PHI.
- ⚡ Even for treatment, payment, or healthcare operations purposes, only the MINIMUM NECESSARY PHI can be accessed. In other words, only the least amount of information that you need in order to perform your job can be accessed.

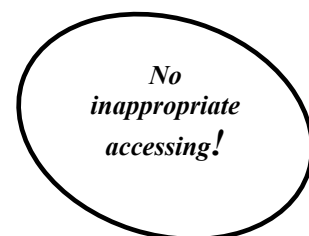
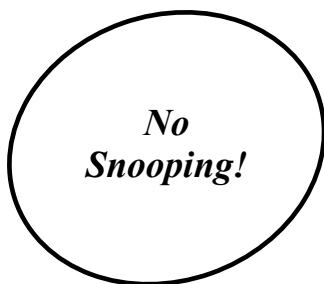
Otherwise, you must have the patient's specific written authorization.

- ◆ **PRIVACY** is expected by the patient regardless of where the patient is obtaining healthcare (a physician's office, a lab, the hospital, etc.). A patient needs to feel comfortable to fully communicate all symptoms, medical history, etc. with providers in order for the provider to best diagnose and treat the patient. If they are concerned about lack of privacy, they may withhold important/vital information. Remember: not only does the patient expect privacy, but maintaining that privacy is a federal law.
- ◆ **INCIDENTAL DISCLOSURES** involve situations in which you accidentally obtain (hear or see) a patient's PHI. An example might be if you overhear a physician speaking to a patient about his/her diagnosis or perhaps a physician talking on the telephone to a consulting physician about a patient's condition. You might accidentally mis-key a patient's encounter number, quickly realize you pulled up the wrong patient's account, and quickly close out. Remember that any PHI you accidentally or incidentally access in situations like this must be kept CONFIDENTIAL.
- ◆ **BREACH OF PHI** is breach of federal laws. This is serious. It can cost you your job! You can also be personally fined by the federal government. You can also be sued by the patient.



There is no way to list all the potential actions that could be considered a breach. Below are some examples, but these examples are definitely not all inclusive. One very important piece of advice is to use common sense.

- ⚡ NEVER intentionally look up information on a patient for personal use or personal interest.
- ⚡ NEVER fall into the trap of having someone else ask you to look up information on a patient. If that person needs to know the information in the performance of his/her job, he/she should have access to it themselves, and should not have to ask someone else to access it for them. People have been terminated (fired) because a co-worker or friend in another department asked him/her to look up something on a patient for their personal information because they knew that person had access to the information.
- ⚡ NEVER take pictures of a patient with your cell phone or by any other personal means. If there is a need to photograph a patient, it must be done with Rush-provided equipment and maintained according to privacy and security regulations.
- ⚡ NEVER put anything relating to patients on social media, like Facebook!
- ⚡ NEVER discuss patient(s) with other staff, unless they have a direct work-related need to know the information.
- ⚡ NEVER discuss patient(s) with family, friends, church members, neighbors or anyone else.
- ⚡ NEVER leave PHI in public areas or in any area in which unauthorized people might be able to see it.
- ⚡ NEVER discuss patient information in public places where your work-related conversation might be overheard by anyone who should not be privy to that information. Beware of elevators, lobbies, hallways, cafeteria, etc.
- ⚡ NEVER put papers with patient's name or other PHI in the regular trash. (This includes IV bag with a label containing a patient's name.)



- ◆ **SECURITY provisions** under HIPAA/HITECH requires that we safeguard all forms of PHI, whether paper or electronic.

Below are just a few examples of reminders. Again, use common sense.

- ⚡ NEVER share your log-on and password with anyone else. Everytime you log on to the computer, it records an audit of what information you accessed and whether you looked at it and/or printed it. You will be held accountable for any PHI accessed under your log on and password.
- ⚡ NEVER use someone else's log-on and password.
- ⚡ NEVER leave your log-on and password written down, where someone else might access it.
- ⚡ CHANGE YOUR PASSWORDS often and do not use passwords that might be easy for co-workers or others to figure out. It is best to use a combination of lower and upper case letters with numbers. Good examples might be c1947RF
- ⚡ NEVER leave your computer without logging off. If you leave your computer and you are still logged in and someone else accesses PHI while you are away, YOU are accountable.
- ⚡ NEVER take any PHI off-premises, even with the best of intention.
- ⚡ NEVER download any PHI or financial information onto any form of media unless you have been granted specific approval by the Executive Compliance Committee, at which time you will be given a secured encrypted device to use.
- ⚡ Always follow the Rush policy/procedure on faxing (it was printed in the September 2012 *Compliance Communicator* and is readily available on Rushnet.)
- ⚡ Always wear your name badge where it is clearly visible to staff and others (i.e picture and name side visible.)
- ⚡ Escort any visitors into areas with PHI (Protected Health Information). Do not allow them access alone.
- ⚡ Remember that YOU can now be held personally liable for a breach.
- ⚡ Thou shall safeguard laptops, computers, smartphones, etc. from easy access to theft.



DISCUSSION QUESTIONS:

1. You work in a hospital and happen to know that Billy Bob was in the Hospital recently because you saw his new girlfriend in the cafeteria and she commented that he was in the ER. That night, you see your cousin (who is Billy Bob's soon to be ex-wife). What do you do?
 - a. You have access to patient records in the normal course of your job; so, you look up Billy Bob's record to see why he was in the hospital, but you don't tell anyone any information you saw. **WRONG!**
 - b. You look up his record, find out why he was here, and tell your cousin that Billy Bob was in the hospital for anxiety and chest pain. It might be useful information to her in her divorce. **WRONG!**
 - c. You do not look up Billy Bob's medical record nor access his information in anyway, and you do not make any comments to anyone. Although you originally found out that Billy Bob was in the hospital from his girlfriend (who doesn't work at the hospital), it is best to "keep you mouth shut", because you don't want even the possible suggestion that you obtained information about patients inappropriately. (It is none of your business.) **RIGHT!**
2. You work in the Emergency Room, and today was a tough day. It was busy your entire shift, and to make matters worse, you had a 6 year old child involved in an accident, bite you and kicked you while you were trying to draw blood.
 - a. You sign on to Facebook that night, read where Susie Q posted seeing an accident that involved a small child. You can imagine it was the same child you had as a patient, so you post "On yah, that kid kicked me and bite me today when I tried to draw blood." **WRONG!**
 - b. You sign on to Facebook that night, read where Susie Q posted seeing an accident that involved a small child. You can imagine it was the same child you had as a patient, so you post "yes, he was brought to the ER, but he is okay and went home". **WRONG!**
 - c. This child has a really bad displaced fracture. His bone was sticking out of his clothes. You pulled out your cell phone and made a picture because you just hadn't seen a case that severe before. Since you are looking at Facebook, and see Susie Q's post about seeing this accident, you think "oh, I'll post the picture of that fracture". **WRONG!**

- d. You sign on to Facebook that night, read where Susie Q posted seeing the accident that involved a small child. You can imagine it was the same child you had as a patient, but you know you cannot make any comment whatsoever about your patient. You certainly don't have any photos on your cell phone because you know this is inappropriate. RIGHT!

For one thing, this accident was in the newspaper and mentioned it was a child involved. Even though you wouldn't have mentioned the patient's name and his face was not in the photo you took (that you shouldn't have taken), many people would be able to relate your comments as to who you were talking about by associating common information from the newspaper article or simply knowledge in the small community that little Jimmy Brown was in an accident this morning.

SUMMARY:

Always do the right thing – even when no one is looking. If you aren't sure what the right thing is, ASK.

If something bothers you, talk with your manager or supervisor. If you don't feel your concern is handled properly, go up the chain of command. You can ALWAYS CALL THE COMPLIANCE OFFICER DIRECTLY (601-703-9493).

Be sure to always identify the patient, effectively communicate with each patient, only charge the patient for the services provided – make sure you are charging the correct patient for the correct items/service and in the correct quantity. Be kind to our patients – without them you wouldn't be here. SERVE others. Appreciate and be kind to teammates and co-workers – makes for a much more pleasant day or night.

Thanks for your compliance!

Cathy Robinson

Rush strives for a Culture of _____.

If you aren't sure how to do something

1. Use your common sense and do the best you can.
2. Ask your supervisor how to correctly perform the task.
3. Just guess.

If you have a concern about whether we are compliant with billing guidelines or coding guidelines or just have a feeling something isn't quite right, you should

1. Keep it to yourself.
2. Bring it to the attention of your supervisor. If you don't receive a response or still have strong concerns after discussing it with him/her, take it up the Chain of Command.
3. If you don't feel comfortable discussing it with your supervisor (or perhaps it involves your supervisor), you can contact the Compliance Officer directly or you can report it anonymously through the external Hotline or the Rushnet Break with the Boss (but be sure to give sufficient details to allow an investigation).
4. # 2 and #3

The Chief Compliance Officer for Rush Health Systems is

1. Eric Holder
2. Tim Tebow
3. Cathy Robinson

The Privacy Officer is

1. Angie Southfork
2. Angie Sherrill
3. Justin Timberlake

You should do right, even when no one is looking!

1. True
2. False

The _____ (3 words) sets the foundation for compliance at Rush Health Systems and its affiliated entities. It covers a range of categories, giving the foundation for how we are to conduct operations at Rush.

Retaliation is

1. Absolutely not allowed
2. Allowed under certain circumstances
3. Depends on who is involved

If we have patients or caregivers of patients who are deaf,

1. They have to call on family members to interpret for them.
2. We have a program in place, administered through the House/Nursing Supervisor to provide needed communication aids and interpretation for the deaf.
3. We try to see if someone around has any knowledge of sign language and use them.

Language Line Services

1. Can be utilized for Spanish speaking patients (who cannot speak or understand English)
2. Can be utilized for French speaking patients (who cannot speak or understand English)
3. Can be utilized via a visual component for sign language interpretation.
4. #1, 2, 3, and 4 are all correct.