HIPAA




Via Christi HEALTH | ASCENSION

Our Mission

Rooted in the loving ministry of Jesus as healer, we commit ourselves to serving all persons with special attention to those who are poor and vulnerable. Our Catholic health ministry is dedicated to spiritually centered, holistic care which sustains and improves the health of individuals and communities. We are advocates for a compassionate and just society through our actions and our words.

Our Values

Service of the Poor

Generosity of spirit, especially for persons most in need

Reverence

Respect and compassion for the dignity and diversity of life

Integrity

Inspiring trust through personal leadership

Wisdom

Integrating excellence and stewardship

Creativity

Courageous innovation

Dedication

Affirming the hope and joy of our ministry

Our Vision

We envision a strong, vibrant Catholic health ministry in the United States which will lead to the transformation of healthcare. We will ensure service that is committed to health and well-being for our communities and that responds to the needs of individuals throughout the life cycle. We will expand the role of laity, in both leadership and sponsorship, to ensure a Catholic health ministry of the future.

Table of contents

This booklet gives you important information about our responsibilities for protecting and safeguarding the Protected Health Information (PHI) of those we serve. Federal and state laws guide our actions. HIPAA (Health Insurance Portability and Accountability Act) is a well-known federal law first passed by the United States Congress in 1996. HIPAA has many parts, but this booklet gives you a basic explanation of the Privacy and Security Rules, and how the law protects the privacy and security of health information. These rules became effective in 2003.

Additionally, the HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009 and the HIPAA Omnibus Rule of 2013 strengthened portions of the Privacy and Security Rules. The state of Kansas also has laws regarding the privacy and security of confidential health information.

This booklet tells you how to report actions that appear to be illegal or not in compliance with our policies. Via Christi welcomes such information and does NOT tolerate retaliation or punishment for the reporting of issues.

Please take the time to read this booklet and to ask any questions you may have about the content. We want you to be informed and involved as we focus on building and maintaining a culture of integrity, openness, transparency and service.

Introduction

Although there are many laws that protect the privacy and security of health information, the healthcare industry often refers to all these rules as "HIPAA compliance." HIPAA stands for "Health Insurance Portability and Accountability Act." It is a federal law first passed by Congress in 1996 that has several parts regarding health insurance reform and health information. In this booklet, we will focus on the parts of HIPAA, as well as other laws, that deal with the privacy and security of Protected Health Information (PHI).

Healthcare organizations must respect the privacy of the individuals they serve and protect the confidentiality of their information. This mandate is more than just the law. It is also a commitment that helps us maintain the trust and loyalty of those persons we serve.

Medical professionals must be vigilant about the correct use and disclosure of health information. We are not allowed to discuss or use protected health information for purposes other than treatment, payment or healthcare operations without the person's authorization, or as allowed by law.

HIPAA compliance also makes good business sense. Our reputation for protecting health information is part of our reputation for quality care. Failure to protect such information can damage our reputation and cause loss of respect in the communities we serve.

The privacy and security of PHI is an important component of the Via Christi Corporate Responsibility Program. We have a Privacy Officer and a Security Officer serving Via Christi. We also have Privacy Officers and Security Officers in all our Via Christi ministry locations. Policies, procedures and the Privacy Officer Manual guide the decisions of our Privacy and Security Officers.

Every Via Christi associate must have a basic understanding of laws concerning the privacy and security of PHI. This even includes those persons who do not have rights to access PHI. And, any of our Business Associates who have access to such information must understand and follow the same rules as we do. Violations can result in large monetary fines for both organizations and individuals. If the violation is severe, it can even lead to imprisonment. Associates may face corrective action up to and including termination for the inappropriate access and disclosure of information. Non-associates may lose access to systems and information for similar violations.

Our Value of Reverence states that we have respect and compassion for the dignity and diversity of life. Showing respect for the privacy of those we serve and ensuring the confidentiality of their health information is another opportunity to express this value in our everyday actions.

HIPAA Privacy Rule

In your role with Via Christi, it is very important that you respect the privacy of those persons we serve and that you have a basic understanding of HIPAA law. The HIPAA Privacy Rule became effective in April 2003. The intent is to protect the confidentiality of individuals' health information, while still allowing sufficient sharing of information to provide quality care to our patients. The Privacy Rule also gives certain rights to persons regarding their health information.

Important definitions

The following definitions will help you to better understand the HIPAA Privacy Rule:

- **HIPAA** — Health Insurance Portability and Accountability Act, a law passed by the United States Congress in 1996.
- **HITECH Act** — Health Information Technology for Economic and Clinical Health, a law passed by the United States Congress in February 2009. This law was a part of the "Stimulus Act" and made some significant updates to the HIPAA law.
- **HIPAA Omnibus Rule** — a final set of regulations updating HIPAA as outlined in the HITECH Act.
- **Covered entity** — an organization required to abide by HIPAA rules. They include healthcare providers such as hospitals, physician practices, nursing homes, pharmacies, dentists, therapists, home health agencies and ambulatory facilities. Also, health plans and healthcare clearinghouses may be covered entities depending on their size. To be a covered entity the organization must also conduct certain transactions electronically.
- **Individually Identifiable Health Information** — any piece of information that could be used to identify a person. Examples include name, Social Security number, street address, medical record number, date of birth and photo.
- **Protected Health Information (PHI)** — individually identifiable information that is used, sent, received or created by a covered entity. It may include demographic, financial and health information about a person. It can take many forms, including written, oral and electronic. HIPAA has strict rules about how PHI can be used and shared both inside and outside a covered entity.
- **Minimum necessary** — the least amount of information that persons need to do their jobs. The Privacy Rule requires that covered entities limit the use and disclosure of PHI to the minimum necessary for the intended purpose.
- **Use of information** — the authorized access of PHI within an organization that maintains the information.
- **Disclosure of information** — the access of PHI outside of the organization maintaining the information.

The Privacy Rule allows covered entities to use and disclose PHI for treatment, payment and certain healthcare operations with a few exceptions. It is helpful to understand the meanings of these three terms:

- **Treatment** — giving, coordinating or managing healthcare and related services. This may include care or service by a healthcare provider, by a healthcare provider along with a third party, by consultations between healthcare providers concerning a patient or the referral of a patient from one healthcare provider to another.
- **Payment** — refers to the many activities of receiving payments or reimbursements for care and service.
- **Healthcare operations** — refers to healthcare activities such as reviewing the competence or qualifications of healthcare providers, conducting healthcare practitioner training programs, accreditation or certification activities, auditing functions, licensing or credentialing activities, medical reviews and legal services.

Workforce responsibilities

What are your responsibilities as part of the workforce?

You have certain responsibilities in your role with Via Christi regarding PHI. You must be aware of these rules, even if you seldom access PHI.

- Access only the information that is needed to do your job. Share with others only the information they need to do their jobs. This is called "minimum necessary."
- Be aware of your surroundings when you are discussing health information with your colleagues. You should not discuss such information in public places where you can be easily overheard, such as elevators, public cafeterias and hallways.

Q&A

Won't the HIPAA Privacy Rule's minimum necessary restrictions hold up the delivery of quality healthcare by preventing or hindering necessary sharing of patient medical information among healthcare providers involved in a person's treatment?

No. Disclosures for treatment purposes between healthcare providers are explicitly exempted from the minimum necessary requirements.

- Never post any type of patient information on social media networks, such as Facebook, Twitter, Linkedin, and any other online platforms.
- Do not leave documents with PHI lying on your desk or in other places where unauthorized persons might see them. When your work is done, put these papers away in a safe location.

- If you print or make copies of confidential information, retrieve the document immediately or use printers and copiers that are located in secure areas.
- Do not leave PHI on a computer screen where unauthorized persons might be able to read it. Log off your computer when you leave your work area.
- Sometimes we are tempted to look at the medical records of family members, friends or even celebrities receiving care in our facilities. DON'T! We are not permitted to do this. In fact, we are not even allowed to access our own medical records. We must follow the process for getting a copy of our medical records.
- Know the procedures in your work area for the shredding of documents. Many areas have containers where you can put documents to be shredded. If you have a shredder in your department, it should be a "confetti, cross-shredder" to meet HIPAA standards.
- Use caution when you are having a phone conversation regarding a person's health condition. Try to be in a private place where others are not able to hear the call or forward the call to a more secure setting.

Q&A

Is it acceptable to discuss information about a patient on my Facebook account as long as I don't disclose any PHI?

No, you should NEVER discuss any type of patient information on Facebook, even if you are not posting any PHI. It can be quite easy for other persons to figure out who you are discussing, plus such actions show a lack of Reverence, one of our Values.

- Close the door or pull the curtain when you are treating a patient or having a discussion regarding a person's medical condition.

The use of electronic mail (email) requires some special precautions.

- When sending an email, give careful thought as to whether or not it is necessary to include PHI. The email could be misdirected, forwarded or printed, resulting in a violation of the HIPAA Privacy Rule.
- If you must put PHI into an email for external distribution, encrypt the email. In most Via Christi ministry locations, this may be done by typing -secure- or -phi- in the subject line. Never include PHI in the subject line of an email. Specific instructions are found on the Source. If you are unsure about the encryption policy for your ministry location, contact your Privacy or Security Officer.
- Verify that you are sending the email to the correct person(s).

Many violations occur as a result of misdirected faxes.

- Verify that you are sending the fax to the correct number and person.
- Use a cover page that includes a confidentiality notice along with your name and phone number so that you can be contacted.
- Make sure that the recipient is authorized to receive the information.
- It is good practice to call and verify that the person received your fax.
- If you are expecting a fax with PHI, have it sent to a secure location or pick it up immediately.
- Audit the fax numbers stored in an automated faxing system on a scheduled basis at least annually.

Q&A

What information can be faxed?

It is okay to fax PHI, but only include the minimum information necessary. The sending of faxes is one area where many violations occur. You should make sure that the fax number is correct and that the information was received by an authorized person. If you are using an automated fax machine, you should review the programmed numbers at least once a year to ensure they are still correct.

What are the responsibilities of Via Christi and its ministries?

Via Christi and its ministries have certain responsibilities regarding the privacy of PHI. These include the following:

- We train all workforce members on privacy policies and procedures.
- Each of our ministries has a Privacy Officer designated to ensure we follow privacy laws, have policies in place, answer questions and investigate potential violations.
- We monitor and audit access to electronic records, to make sure that persons are not reading or using PHI for inappropriate reasons.
- We respect the rights of persons we serve regarding their health information, and we respond to any complaints they may have.
- We give persons a notice of our privacy practices. This tells people how we use and disclose their PHI, the rights they have under the law and our legal duties. We hand out this notice to every person at the time of a first visit to receive medical care.
- We restrict access to electronic PHI through the use of logins and passwords.

Individual rights

What are the rights of individuals with respect to their Protected Health Information?

- **The right to access one's own record —** HIPAA gives persons the right to read and receive a copy of their health information maintained by a covered entity. They may look at their medical records, billing records and any other information used to make medical decisions.

  There are some exceptions to the right of examining one's own PHI. A covered entity does not have to share psychotherapy notes or information being compiled in reasonable anticipation of a lawsuit.

  If the individual was part of a research study and agreed to restricted access as part of the study, PHI does not have to be shared with the person. If a licensed healthcare professional believes that the sharing of PHI might put the individual or anyone else in danger or risk of harm, the covered entity is not required to provide the information. If the decision is based on this reason, the person may appeal.

Q&A

I was caring for a patient who has been moved to another unit. Am I permitted to look at the individual's medical record?

If there is not a legitimate reason, such as treatment, for you to access the record, then you are not allowed to view the patient's information.

- **The right to request change to one's own record —** There may be instances when an individual believes that the information in his or her medical record is inaccurate or incomplete. A person has a right to ask that the record be amended.

  Covered entities are not required to make changes to a person's medical record. If it is determined that the record is complete and accurate, the request for amendment may be denied. If the information to be changed was not created by the covered entity, the request may be denied. As a general rule, a medical record should not be changed in such a way that completely eliminates the original information.

- **The right to request additional restrictions —** Persons have the right to ask for additional restrictions on the use and disclosure of their PHI. However, covered entities do not have to agree to such requests. If a covered entity does agree to such a request, it is required to do so completely and to keep records of its compliance with the restriction.

The HIPAA Omnibus Rule has updated this law. If a person completely pays for a medical service out of his/her own pocket and asks that this NOT be shared with the person's health plan, the covered entity must abide by this request.

Q&A

Does the HIPAA Privacy Rule allow a healthcare provider to leave a message on a patient's answering machine?

Yes, this is permitted. However, covered entities should take care in the amount of information disclosed in the message. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

- **The right to confidential communications —** A person has the right to ask the covered entity to communicate in a certain way. For example, a patient may ask the doctor to leave a voice mail at a certain phone number. The covered entity must abide by such requests as long as they are reasonable.
- **The right to know who has received one's PHI —** HIPAA gives persons the right to find out who has received their PHI. This is called an "accounting of disclosures." In the event a person asks for this information, a covered entity must be prepared to give a listing of disclosures it has made during the past six years. The covered entity does not have to include information disclosed for treatment, payment or business operations.
- **Fundraising and marketing —** HIPAA has several rules about the use of PHI in marketing and fundraising communications. If you are responsible for the marketing of Via Christi products or services, or you are involved in fundraising activities, you must work with the Marketing Department and your Privacy Officer to ensure you are in compliance with the law.

Q&A

Do the minimum necessary requirements prohibit medical residents, medical students, nursing students and other trainees from accessing patient medical information in the course of their training?

No, this is not prohibited. Healthcare operations include "conducting training programs in which students, trainees or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers."

HIPAA Security Rule

The HIPAA Security Rule became effective in April 2003. The Security Rule states that we must have policies and safeguards in place to protect PHI in electronic format. This is often referred to as EPHI (Electronic Protected Health Information). We must protect our computer systems against unauthorized access to make sure EPHI is not destroyed, lost or accessed by someone not allowed to do so. We must also ensure that EPHI is reliable and readily available to those persons needing this information to fulfill their job responsibilities.

Workforce responsibilities

What are your responsibilities as part of the workforce?

You may have a personal desktop or laptop computer assigned to you, or you may share a computer with other persons in your work area. When using a Via Christi computer, there are guidelines for protecting EPHI.

Passwords

A password is the key that you need to access the information stored on our computer systems. It should be protected in the same way that you protect the key to your house or your car. You should NEVER share your passwords with anyone, even if doing so might save time or avoid some inconvenience.

When you leave your house, you don't leave the door open. In the same way, when you leave your computer, you should always lock or log off. If someone else uses your computer account in an inappropriate or illegal manner, you could be held responsible for the other person's activity. Do not ask others if you can use their IDs and passwords. Your account is set up to give you access to the information you need to get your job done.

If another person logs into your account, he or she might delete or change your computer data, accidentally or intentionally. It could be embarrassing if someone sends an inappropriate email message or browses improper web sites using your name. Sharing your password is a violation of Ascension HIPAA security policies.

It is important that you change your passwords on a regular basis. Many Via Christi applications force you to change your passwords every ninety (90) days. Any time that you believe a password has been compromised, change it immediately. Do not write your password on a sticky note or a piece of paper where it is easily seen or found.

When you log in to some programs and Internet sites, you will be asked if you want your computer to remember your password. This might save you some time, but it is risky. Other persons could access these sites or programs from your computer without knowing the password.

Strong passwords

Choose your passwords carefully. Do not pick ones that are easy to guess, such as the names of your children or pets. There are some techniques you can use to strengthen your passwords and make them more difficult to guess:

- Avoid using words that are found in the dictionary without adding characters or changing them in some way.
- Use at least eight characters in your password.
- Do not reuse the same password.
- Use a variety of characters, including upper and lower case alphabetical, numeric and other keyboard symbols such as exclamation points.

Password tricks and tips

It is sometimes difficult to remember passwords. There are some tricks you can use to make it easier. You might select two activities or two movies that you enjoy and join them together with a symbol, such as GWTW&Titanic (Gone with the Wind and Titanic). In some cases, you can substitute numbers or symbols for letters. An outdoor enthusiast might use 2Boat&Fish or 2B0at&F!sh.

Another good way to remember a password is to base it on a phrase. For example, the phrase "crime never pays" may remind you that your password is Cr1me_NP. Capital letters have been mixed into this password, and the numeral 1 is used in place of the letter i.

If you must write down your password, use a reminder instead of the actual password. You could invent a name and address and include it in your address book, such as:

Harold Smith
1090 St. Joseph Street
Wichita, KS
This could be a reminder for the password HS1090KS.

Q&A

Is it OK to use an associate's password to look up some information that I need to do my job?

No, it is NEVER OK to use another person's password or to let someone else use your password. It could be embarrassing or even worse if someone behaves inappropriately while logged into your account. If you have forgotten your password, call Ascension Information Services at 877.640.1418.

Malicious software (or malware)

We must be alert for software or computer programs that are installed on our computers without our knowledge, possibly causing a variety of problems. These programs are called malicious software, or malware, and there are several categories:

Viruses

One type of malicious software is a computer virus, a program that is designed to copy itself and spread from computer to computer.

Viruses may cause a variety of problems including:

- Slow computer performance
- Destruction of computer files
- Loss of productivity
- Theft of data stored on a computer (passwords, account information, etc.)

Viruses are usually spread by one of the four following methods:

- Email attachments
- Data CDs, USB (thumb) drives and floppy disks
- Internal network
- Direct Internet connection

Q&A

Via Christi has assigned a laptop computer for my use. Is it acceptable for me to store PHI on the hard drive of the laptop?

It is best NOT to store any type of PHI on the local hard drive of a computer or on a removable flash drive. Such information should be stored on a network server if at all possible. However, if this is required for a business related activity, you should ensure that your laptop or thumb drive has encryption software installed. If you are not sure or need to have this done, contact Ascension Information Services. In fact, all laptop computers are required to have encryption software installed to secure them from unauthorized access.

The most common way that computer viruses spread is through email attachments. Be cautious when you receive an email with an attachment, especially if you do not know the sender or were not expecting the email. If you receive a message with an attachment you were not expecting or cannot check with the sender to make sure he or she meant to send it, you should delete it. If you were expecting the attachment or can verify with the sender, it is probably safe to open the attachment. Do not open files with these extensions unless you were expecting the attachment.

Be careful with files that have the following extensions after the filename:

.bat	**.exe**
.com	**.hlp**
.lnk	**.scr**
.pif	**.vbs**

You should never open an attached file if it has a double extension, for example: .vbs.jpg.

If you are not sure or have concerns about opening an attachment, do not hesitate to call Ascension Information Services (AIS) for assistance.

Viruses also spread via thumb drives and data CDs. If someone gives you a drive or CD, it is a good idea to check it for viruses first. Plug or insert the device into your computer and scan it using your antivirus software. If a virus is detected, call AIS or your System Administrator.

Computers may also be infected with viruses through connection to a network or to the Internet. All Via Christi computers should have antivirus software installed to help decrease the risk of this happening. We also have firewalls in place to protect against Internet viruses. However, even with these safeguards in place, we must still be cautious and vigilant. New viruses are constantly being introduced and can sometimes sneak in before the antivirus software is prepared to deal with them. If you ever suspect that a virus has been copied to your computer, take the following steps:

- Physically turn off the computer.
- Contact AIS or your System Administrator immediately.
- If you suspect a virus on your computer at home that is used to access the Via Christi network, do not connect until the problem is resolved. You can look at the website of your antivirus software vendor to get information on dealing with the virus.

The best defense against a computer virus is YOU, the computer user. Make sure that you have antivirus software installed on your computer and that it is always running. Make sure that it is updated on a regular basis to protect against the newest viruses. Also, be sure to back up any critical files. Files stored on Via Christi network drives are backed up nightly.

Q&A

I sometimes receive emails from friends or family asking me to forward the message to others in my address book. The emails are usually harmless, sometimes funny and sometimes inspiring. Is it acceptable to pass these along?

Everyone has probably received this type of email at one time or another. The best practice is to delete these, even if they appear harmless. Some emails may be hiding malicious software, such as viruses. Even if they do not, just the process of many persons forwarding such emails can flood the computer network with unnecessary data and cause everything to slow down.

Spyware

Spyware is another type of malicious software. This is software that is often secretly installed on a computer for the purpose of gathering information about the user. This may happen when software is being downloaded from the

Internet. It can cause problems such as slow computer performance, unwanted pop-ups while Internet browsing and even system failures.

Spyware takes more time and energy from an IT department than any other single computer issue. It may directly compromise our compliance with HIPAA, because it often interferes with the availability of patient information on affected computers.

We strictly prohibit downloading software from the Internet. If this is required for business-related purposes, it may be requested through AIS.

Trojan horses

Trojan horse programs are similar to spyware. The computer user may be asked to download or install a program that appears to be safe, but a harmful program (Trojan horse) is hidden within the safe program. These are most often spread through Internet downloads and are hidden from the user until they start causing harm to the computer.

Social engineering

A "Social Engineering" attack happens when someone tries to trick you into revealing information that can then be used in a harmful way. Here are some examples:

- A person calls you and pretends to work for the AIS Service Center or system administration. The person asks you to confirm your password or reset your password. Verify the person's identity by asking for a callback number. Most criminals will not provide a callback number.
- You receive a phony email asking you to go to a website where you are directed to enter personal information, such as your Social Security number or a bank account number. Never click on an email asking for verification of personal information or account information. Instead, type the website address in the browser directly. Computer hackers sometime create phony websites that are identical in appearance to a major corporate website in order to obtain information from unsuspecting persons.
- Do not access social media networks such as Facebook, Twitter, YouTube and similar sites while working one's assigned shift unless there is a business-related reason for such access and the associate's senior administrator has given approval. This includes access using either the Via Christi computer network or the guest network.

Physical security

Our Standards of Conduct state that we protect our assets, both the property and information entrusted to us by Via Christi. This is important for many reasons, including the protection of confidential health information. Follow these guidelines to ensure the physical security of our EPHI:

- If at all possible, do not store EPHI on electronic devices that may be easily misplaced or stolen. These include USB (thumb) drives, CDs, laptop computers and mobile devices. The theft or loss of such devices containing EPHI can result in large fines and bad publicity.
- If you must store EPHI on any type of portable electronic device, the device must be encrypted and password protected.
- Lock up electronic devices when they are not in use. Do not leave laptop computers in your vehicle. Most losses experienced by Via Christi are due to laptops stolen from vehicles.
- If you are throwing away any storage devices or removable media, be sure any EPHI is removed per HIPAA standards. If you are not familiar with these standards, talk to the Security or Privacy Officer.
- If you see an unfamiliar person in your work area, do not hesitate to ask the purpose of the visit. This is especially true if the individual is not wearing an associate or vendor badge.
- Become familiar with the security policies adopted by your ministry.
- Associates use the Via Christi network to access computer applications and Internet sites during their work shifts. Associates do not use other networks, including the guest network, unless such access is required for a business-related function and has been approved by a member of management.

Q&A

I am a patient at a Via Christi ministry location and want to check on my own personal medical record. This is my information, so isn't it okay to look at this with out anyone's approval?

No, you may not access your own record without following the same steps required for all patients. This would be a violation of Via Christi policy.

Via Christi responsibilities

What are the responsibilities of Via Christi and its ministry locations?

Via Christi and its ministries have certain responsibilities regarding the security of PHI. These include the following:

- We train all workforce members on security policies and procedures.
- Each of our ministry locations has a Security Officer designated to ensure we follow the HIPAA Security Rule, have policies in place, answer questions and investigate potential violations.
- We monitor and audit our processes concerning the security of EPHI.

- Copiers and multipurpose units we use for copying, printing, scanning and faxing may have built-in electronic storage devices. We ensure that any information stored on these devices is erased prior to returning them at the end of lease.
- We respect the rights of those persons we serve regarding their health information, and we respond to any complaints they may have.
- We have controls in place to ensure the security, integrity and availability of EPHI including, but not limited to, the following:
  - Required passwords
  - Forced password changes
  - Antivirus software
  - Firewalls
  - Spam filters
  - Encryption
  - Installing software updates and patches
  - Backup processes
  - Environmental controls
  - Maintenance contracts on hardware and software
  - Disaster recovery plan
  - Blocking of inappropriate websites
  - Badges for authorization to enter secured locations
  - Management authorization required for computer system access
- We have policies and procedures in place to ensure EPHI is readily available to those persons requiring access in order to fulfill their job responsibilities.

Q&A

Is a photo considered protected health information?

Yes. Any photo that includes a person's face or could be used to identify a person is PHI.

Penalties for non-compliance with HIPAA

There are different levels of civil penalties for violating the HIPAA regulations. Monetary fines can be anywhere from $100 per violation to $1.5 million during a calendar year depending upon the nature of the violation.

There are also criminal penalties for severe violations of HIPAA law, resulting in both fines and imprisonment up to 10 years. Both organizations and individuals can be found guilty of HIPAA violations.

Associates of Via Christi can face corrective action up to and including termination. We may revoke access to computer systems and information in any format to non-associates for similar violations. Failure to comply with HIPAA can be expensive and damaging.

Reporting compliance concerns

Problems cannot be fixed if we do not know about them. You have a duty to ask questions and report in good faith concerns related to your workplace. There are several ways in which you can ask a question or share a concern:

- Discuss any potential issue with your immediate supervisor or that person's supervisor; or
- Contact the Corporate Responsibility Officer, Privacy Officer or Security Officer for your respective ministry location; or
- Contact the Via Christi Corporate Responsibility and Privacy Officer:

  Sara Powers
  8200 E. Thorn
  Wichita, KS 67226
  Phone: 316-858-4978; or
- Contact the Via Christi Health Security Officer:

  Keith Ashpole
  3720 E. Bayley
  Wichita, KS 67218
  Phone: 316-350-3822; or
- Call the Values Line, 800-794-9027 or access at ascensionhealthvaluesline.org. When you call the Values Line, your report will be confidential. A third party will talk to you about your concerns. You will receive a report number. We will investigate your concerns and provide a prompt response through the service. If you leave an anonymous message, please report enough facts to allow us to investigate your concern.
- Via Christi does not allow retaliation against you for reporting your concerns.

Conclusion

Every one of us is responsible for protecting the privacy and security of health information for those persons we serve. We must follow the policies and procedures designed to ensure compliance with HIPAA Privacy and Security regulations and all other applicable federal and state laws. Each of us has an important role to play as we carry out our day-to-day job responsibilities.

As we strive to create a culture of honesty and integrity, we must incorporate a respect for the privacy of our patients and residents, and concern for the security of their protected health information. This is not just law; it is also an ethical obligation on our part and the right of every person we serve.

Via Christi Health
8200 E. Thorn
Wichita, KS 67226

viachristi.org

Via Christi HEALTH | ASCENSION

Via Christi offers a continuum of care from the birth of a child to enhancing the lives of older adults. This program or service is part of Via Christi.

Via Christi is an Equal Opportunity (EOE) and Affirmative Action Employer. We support diversity in the workplace.