

SARATOGA COUNTY PUBLIC HEALTH NURSING SERVICE

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO YOUR PROTECTED HEALTH INFORMATION.

PLEASE REVIEW THIS NOTICE CAREFULLY

Saratoga County Public Health Nursing Service is committed to maintaining the confidentiality of your Protected Health Information (PHI). In providing your care, we will create records regarding your treatment and the services we provide to you. We are required by law to maintain the confidentiality of your Protected Health Information.

This notice will provide you with information on how we may use and disclose your Protected Health Information.

This notice applies to all records maintained by this agency containing your Protected Health Information. We reserve the right to revise or amend this privacy notice. Any changes will be effective for Protected Health Information we maintain about you at that time. Our agency will post a copy of our revised notice in our office and you may request a copy by calling our office at (518) 584-7460.

If you have questions regarding this notice, you may contact the HIPAA Compliance Office at (518) 584-7460 during normal business hours.

WAYS WE MAY BE USING AND DISCLOSING YOUR PROTECTED HEALTH INFORMATION

The following are ways in which we may use and disclose your Protected Health Information:

TREATMENT: Our agency may use your PHI to provide treatment to you. We may allow or disclose information to agency nurses access to your medical record to provide ordered care. In addition, we may disclose information to others who may assist in your care such as therapist and home health aides and home health aide agencies.

PAYMENT: Our agency may use and disclose PHI for billing and payment for services and supplies you may receive. Examples of such use and disclosure may include: contacting your health insurance provider to verify coverage and to obtain payment. We may also release information to you or other third party individuals to obtain payment.

HEALTH CARE OPERATIONS: Our agency may use and disclose your PHI to conduct business. For example we may use and disclose your information to evaluate the quality of care you received or monitor our compliance with state and federal regulations.

APPOINTMENT REMINDERS: Our agency may use and disclose your PHI to contact you to remind you of visits and/or appointments.

BUSINESS ASSOCIATES: Our agency may use or disclose information to a person or entity we contract with to perform some of our functions for us and who need access to the information to perform those functions. For example: a billing service, attorney, and auditor.

HEALTH RELATED BENEFITS: Our agency may use or disclose your PHI to facilitate your discharge.

RELEASE OF INFORMATION TO FAMILY/FRIENDS: Our agency may use or disclose your PHI to a friend or family member that is assisting in your care or helping you pay for your health care.

USES AND DISCLOSURES OF PHI WITHOUT AN AUTHORIZATION: Our agency may use or disclose your PHI as required by law and by government agencies, such as to respond to a court order or subpoena and for public health information.

USES AND DISCLOSURES OF PHI WITH AN AUTHORIZATION: In addition, our agency will obtain a signed authorization for any uses or disclosures not for treatment, health care operations, and payment and will use the information as stated in the authorization. All such requests will be looked at on a case-by-case basis to limit the release of information to the minimum amount necessary. You have the right to cancel an authorization at any time, except to the extent that this agency or another company or individual has already relied on the information.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION (PHI): You have the following rights regarding the PHI that our agency maintains about you. You may contact the agency's HIPAA Compliance Coordinator at (518) 584-7460 to obtain the appropriate form needed to exercise any of these rights.

CONFIDENTIAL COMMUNICATIONS: You have the right to request our agency to communicate with you about your PHI in a particular manner or at a certain location. You must make such a request in writing to the agency HIPAA Compliance Coordinator. We will respond to you in writing within 30 days of receiving your written request.

REQUESTING RESTRICTIONS: You have the right to request a restriction on the uses and disclosure of your PHI. We are not required to agree with your request. You may make your request in writing to the agency's HIPAA Compliance Coordinator.

RIGHT TO INSPECT AND COPY YOUR PROTECTED HEALTH INFORMATION (PHI): You have the right to inspect and obtain copies of your PHI in your medical record. Medical records are the property of this agency. You must make your request in writing to the agency's HIPAA Compliance Coordinator. You may inspect your record within 48 business hours of receipt of your request. Our agency may charge a fee for the cost of copying and postage. You will be informed of the amount prior to the copying. Our agency may deny your request. We will inform you in writing of the reason for the request denial.

RIGHT TO AMEND YOUR PROTECTED HEALTH INFORMATION (PHI): You have the right to ask us to amend your health PHI if you believe it is incorrect or incomplete. You must specify who made the entry, date of entry, reason for change and what it should read. You may request a "Request for Amendment of Medical Record" form from the agency HIPAA Compliance Coordinator. We will respond to you within 60 days of receipt of your written request. If we approve your request we will make the change to your PHI and inform you of the change in writing. Our agency may deny your request if your PHI is accurate and complete; not created by our agency; not part of the PHI kept by us; or not allowed to be disclosed. You will receive written notification of the reason for the denial and will become part of your agency record.

RIGHT TO ACCOUNTING OF DISCLOSURES: You have the right to request a list of situations in which our agency has given out your PHI. The list may not include: disclosures we made so that you could receive treatment; disclosures made to receive payment for the care we provided to you; disclosures made in order to operate our business; disclosures made to you or people you choose; disclosures to law enforcement or authorized governmental agencies; disclosures made prior to April 14, 2003; or disclosures made in accordance with your authorization. You must submit a written request to the agency HIPAA Compliance Coordinator. We will respond within 60 days of receipt of your written request. Your request must state a time period that may not be longer than 6 years and not include dates prior to April 14, 2003. The list will include: date of the disclosure to person/agency disclosed to; description of information; and reason for disclosure. The first list you request within a 12-month period will be free. If you request another list within the same 12-month period, you may be charged a fee. You will be informed in advance of the fee and you will be given a chance to cancel or change your request.

RIGHT TO A COPY OF OUR NOTICE OF PRIVACY PRACTICES: You have a right to a copy of our Notice of Privacy Practices at any time. You may request a copy from the agency's HIPAA Compliance Coordinator at (518) 584-7460.

RIGHT TO FILE A COMPLAINT: If you believe your privacy rights have been violated, you may file a written complaint to the agency's HIPAA Compliance Coordinator at:

**Saratoga County Public Health Nursing Service
31 Woodlawn Avenue, Suite 1, Saratoga Springs, NY 12866-2198**

You may also file a complaint with the Office of Civil Rights, US Department of Health and Human Services. You will not be penalized for filing a complaint.

INCIDENTAL USES AND DISCLOSURES

[45 CFR 164.502(a)(1)(iii)]

Background

Many customary health care communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which individuals receive health care or other services from covered entities, the potential exists for an individual's health information to be disclosed incidentally. For example, a hospital visitor may overhear a provider's confidential conversation with another provider or a patient, or may glimpse a patient's information on a sign-in sheet or nursing station whiteboard. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices and, thus, does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Privacy Rule permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

How the Rule Works

General Provision. The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied *reasonable safeguards* and implemented the *minimum necessary standard*, where applicable, with respect to the primary use or disclosure. See 45 CFR 164.502(a)(1)(iii). An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.

Reasonable Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c). It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

Many health care providers and professionals have long made it a practice to ensure reasonable safeguards for individuals' health information – for instance:

- By speaking quietly when discussing a patient's condition with family members in a waiting room or other public area;
- By avoiding using patients' names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;
- By isolating or locking file cabinets or records rooms; or
- By providing additional security, such as passwords, on computers maintaining personal information.

Protection of patient confidentiality is an important practice for many health care and health information management professionals; covered entities can build upon those codes of conduct to develop the reasonable safeguards required by the Privacy Rule.

Minimum Necessary. Covered entities also must implement reasonable minimum necessary policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures also reasonably must limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business. The minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes. For example, a physician is not required to apply the minimum necessary standard when discussing a patient's medical chart information with a specialist at another hospital. See 45 CFR 164.502(b) and 164.514(d), and the fact sheet and frequently asked questions on this web site about the minimum necessary standard, for more information.

An incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is not permitted under the Privacy Rule.

For example:

- The minimum necessary standard requires that a covered entity limit who within the entity has access to protected health information, based on who needs access to perform their job duties. If a hospital employee is allowed to have routine, unimpeded access to patients' medical records, where such access is not necessary for the hospital employee to do his job, the hospital is not applying the minimum

necessary standard. Therefore, any incidental use or disclosure that results from this practice, such as another worker overhearing the hospital employee's conversation about a patient's condition, would be an unlawful use or disclosure under the Privacy Rule.

INCIDENTAL USES AND DISCLOSURES

Frequently Asked Questions

Q: Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

A: Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an

emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

Q: Does the HIPAA Privacy Rule require hospitals and doctors' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?

A: No, the Privacy Rule does not require these types of structural changes be made to facilities.

Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule. The Department does not consider facility restructuring to be a requirement under this standard.

For example, the Privacy Rule does not require the following types of structural or systems changes:

- Private rooms.
- Soundproofing of rooms.
- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
- Encryption of telephone systems.

Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered entities also may take into consideration the steps that other prudent health care and health information professionals are taking to protect patient privacy.

Examples of the types of adjustments or modifications to facilities or systems that may

constitute reasonable safeguards are:

- Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.
- In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers may constitute a reasonable safeguard. For example, a large clinic intake area may reasonably use cubicles or shield-type dividers, rather than separate rooms, or providers could add curtains or screens to areas where discussions often occur between doctors and patients or among professionals treating the patient.
- Hospitals could ensure that areas housing patient files are supervised or locked.

Q: May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?

A: Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. 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.

A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual's care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed. See 45 CFR 164.510(b)(3).

In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, the Department considers a request to receive mailings from the covered entity in a closed

envelope rather than by postcard to be a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests, absent extenuating circumstances. See 45 CFR 164.522(b).

Q: May physicians offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

A: Yes. Covered entities, such as physician's offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).

Q: Are physicians and doctor's offices prohibited from maintaining patient medical charts at bedside or outside of exam rooms, or from engaging in other customary practices where the potential exists for patient information to be incidentally disclosed to others?

A: No. The HIPAA Privacy Rule does not prohibit covered entities from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual's privacy while engaging in these practices. Covered entities must implement reasonable safeguards to protect an individual's privacy. In addition, covered entities must reasonably restrict how much information is used and disclosed, where appropriate, as well as who within the entity has access to protected health information. Covered entities must evaluate what measures make sense in their environment and tailor their practices and safeguards to their particular circumstances.

For example, the Privacy Rule does not prohibit covered entities from engaging in the following practices, where reasonable precautions have been taken to protect an individual's privacy:

- Maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., "high fall risk" or "diabetic diet") at patient bedside or at the doors of hospital rooms.

Possible safeguards may include: reasonably limiting access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by.

- Announcing patient names and other information over a facility's public announcement system.

Possible safeguards may include: limiting the information disclosed over the system, such as referring the patients to a reception desk where they can receive further instructions in a more confidential manner.

- Use of X-ray lightboards or in-patient logs, such as whiteboards, at a nursing station.

Possible safeguards may include: if the X-ray lightboard is in an area generally not accessible by the public, or if the nursing station whiteboard is not readily visible to the public, or any other safeguard which reasonably limits incidental disclosures to the general public.

The above examples of possible safeguards are not intended to be exclusive. Covered entities may engage in any practice that reasonably safeguards protected health information to limit incidental uses and disclosures.

Q: A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the HIPAA Privacy Rule allow the clinic to continue this practice?

A: Yes, the Privacy Rule permits this practice as long as the clinic takes reasonable and appropriate measures to protect the patient's privacy. The physician or other health care professionals use the patient charts for treatment purposes. Incidental disclosures to others that might occur as a result of the charts being left in the box are permitted, if the minimum necessary and reasonable safeguards requirements are met. See 45 CFR 164.502(a)(1)(iii). As the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to the examination, the minimum necessary requirement would be satisfied. Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing

the wall rather than having protected health information about the patient visible to anyone who walks by. Each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances. See 45 CFR 164.530(c).

Q: A hospital customarily displays patients' names next to the door of the hospital rooms that they occupy. Will the HIPAA Privacy Rule allow the hospital to continue this practice?

A: The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure—for example, the disclosure to other patients in a waiting room of the identity of the person whose name is called. In this case, disclosure of patient names by posting on the wall is permitted by the Privacy Rule, if the use or disclosure is for treatment (for example, to ensure that patient care is provided to the correct individual) or health care operations purposes (for example, as a service for patients and their families). The disclosure of such information to other persons (such as other visitors) that will likely also occur due to the posting is an incidental disclosure.

Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate. See 45 CFR 164.502(a)(1)(iii). In this case, it would appear that the disclosure of names is the minimum necessary for the purposes of the permitted uses or disclosures described above, and there do not appear to be additional safeguards that would be reasonable to take in these circumstances. However, each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances.

Q: May mental health practitioners or other specialists provide therapy to patients in a group setting where other patients and family members are present?

A: Yes. Disclosures of protected health information in a group therapy setting are treatment disclosures and, thus, may be made without an individual's authorization. Furthermore, the HIPAA Privacy Rule generally permits a covered entity to disclose protected health information to a family member or other person involved in the individual's care. Where the individual is present during the disclosure, the covered entity may disclose protected health information if it is reasonable to infer from the circumstances that the individual does not object to the disclosure. Absent countervailing circumstances, the individual's agreement to participate in group therapy or family discussions is a good basis for inferring the individual's agreement.

Q: Are covered entities required to document incidental disclosures permitted by the HIPAA Privacy Rule, in an accounting of disclosures provided to an individual?

A: No. The Privacy Rule includes a specific exception from the accounting standard for incidental disclosures permitted by the Rule. See 45 CFR 164.528(a)(1).

Q: Do the HIPAA Privacy Rule's provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?

A: No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff. For example:

- A provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room.
- A health plan employee discussing a patient's health care claim on the phone may be overheard by another employee who is not authorized to handle patient information.

If the provider and the health plan employee made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.

Q: Is a covered entity required to prevent any incidental use or disclosure of protected health information?

A: No. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures. See 45 CFR 164.530(c)(2).

SARATOGA COUNTY PUBLIC HEALTH NURSING SERVICE HIPAA COMPLIANCE TRAINING

Effective April 14, 2003, the Privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) will become the LAW of the land. This is mandated by Congress, developed by the Department of Health and Human Services, and will be enforced by the Office of Civil Rights. It is the single most significant piece of federal legislation affecting the health care industry and the protection of patient's health and demographic information. This information is known as Protected Health Information of PHI. Civil penalties may arise from violations of the Act and can range from \$100 - \$25,000. Willful violations may result in fines up to \$25,000 and/or ten years' imprisonment.

HIPAA requires certain entities that maintain PHI to implement measures to maintain the confidentiality of such information. Saratoga County Public Health Nursing Service (SCPHNS) is one of those entities.

All agency employees need to be aware that the Saratoga County Board of Supervisors is committed to being compliant with HIPAA. As such, employees also need to be committed to learn and implement the safeguards and policies that have been developed by the County and SCPHNS. This training session is the beginning of a continuing effort to educate and make routine the habit of maintaining the confidentiality of PHI and help the agency improve operations to maintain all PHI securely.

KEY POINTS TO REMEMBER:

1. The Director of Public Health (DPH) has been appointed the HIPAA Compliance Coordinator for the agency. The duties of the Compliance Coordinator can be found in the SCPHNS HIPAA Policy and Procedure document.
2. As part of the training, employees will receive the following:
 - A. The Saratoga County HIPAA Policy and Procedure document adopted by the Saratoga County Board of Supervisors by Resolution 65 of 2003;
 - B. The SCPHNS HIPAA Procedure for Access, Use, and Disclosure of Individually Identifiable Health Information document; and
 - C. SCPHNS "NOTICE OF PRIVACY PRACTICES."Employees should familiarize themselves with these documents and keep them handy for reference. If you have any questions, please contact the Director of Public Health.
3. Employees will acknowledge receipt of these documents and training in writing and the Compliance Coordinator will keep such acknowledgements on file.
4. HIPAA regulations require that SCPHNS provide reasonable safeguards that will protect PHI against uses and disclosures not permitted under the Privacy rule of the Act and that limit incidental uses and disclosures.

5. All areas of the agency will need to modify behaviors as to how and where we discuss PHI. We also need to modify how we transport and store PHI.
6. Areas that need to be focused on and/or modified:
 - A. All doors to rooms need to be closed at all times so that people in the hallways cannot hear conversations that may contain PHI.
 - B. Clinic room doors are to be closed at all times to protect patient confidentiality.
 - C. Avoid discussing PHI in the hallways or areas where public have access.
 - D. Filing PHI in charts and placing charts in file cabinets when not in use.
 - E. Avoid having computer screens visible to the public.
 - F. When transporting PHI, all documents are to be placed in a box and secured in the trunk of the car. The only PHI you should have with you inside the car is the PHI on the next patient you are to visit. This is so you have reference to directions. The vehicle should be locked at all times. If your car does not have a trunk, PHI should be placed in a box and secured within the vehicle.
7. HIPAA allows for the incidental use and disclosure of PHI to occur when reasonable safeguards are in place. Attached is a Q & A section on "Incidental Uses and Disclosures" for your review.
8. Patients have the right to request and inspect and/or copy their medical record. Such requests need to be made per agency policy. Patients also have the right to ask that their medical record be amended. This request does not have to be granted.

REMEMBER
WATCH WHAT YOU SAY –
WHERE YOU SAY IT –
TO WHOM YOU SAY IT

HIPPA TRAINING OUTLINE

I WHAT IS HIPAA?

- A. HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT**
 - 1. Passed by Congress 1996
 - 2. Privacy regulations passed 2002
 - 3. Implementation, April 14, 2002
- B. PRIVACY RULE – Federal privacy protections for individually identifiable health information, a.k.a. protected health information.**
 - 1. regulates entities that deal with PHI
 - 2. gives individuals rights with respect to their PHI
- C. FINES – up to \$50,000 for violation**

II WHAT IS PHI?

- A. Medical Records – clinical records, lab tests, nurses notes, medical reports etc.**
- B. Billing Information**
- C. Identifiable to individual**

III WHAT IS REGULATION SUPPOSED TO DO?

- A. enables individuals to find out how their PHI may be used, to discover how it has been used.**
- B. limits use and transmission of PHI to minimum necessary**
- C. enables individuals to control use and disclosure**

IV WHAT DOES REGULATION REQUIRE?

- A. Entities must have a Policy and Procedure**
- B. Entities must notify individuals of their rights**
- C. Entities must limit their disclosures to the minimum necessary**
- D. Entities must implement their procedures to fulfill individuals' rights**

V POLICY & PROCEDURE

- A. COUNTY POLICY – general – Enacted February 2003**
 - 1. Appoints Personnel Director as Administrator and creates Privacy Officer and Security Officer.
 - 2. Requires department policy for departments handling PHI, and requires department HIPAA Coordinators.
 - 3. Requires contracts – Business Associate Agreements with vendors who will be handling PHI.
 - 4. Requires Training
 - 5. Makes violation of Policy & Procedure illegal behavior subject to County's disciplinary procedures.
- B. DEPARTMENT POLICY**
 - A. Names HIPAA Coordinator for Department – responsible for HIPAA compliance and procedures within department.**

- B. Authorizes employees within Department to handle specific PHI for specific purposes.
 - 1. unauthorized employees would be in violation of policy and subject to discipline.
- C. Identifies routine and recurring transfers of PHI
- D. Requires secure storage and handling of PHI
 - 1. locked filing cabinets or storage rooms
 - 2. passwords and physical care for computers
- E. Specific procedures for handling individual rights

VI WHAT IS MINIMUM NECESSARY STANDARD?

- A. Required by Federal Law and by County and Department Policy
- B. Federal reg – “A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made....
- C. Means use or disclose only that much of a person’s PHI that is needed for that transaction
 - 1. e.g. – billing – does payor need entire medical record?
- D. Fed reg “...A covered entity may not use, disclose or request an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.”
- E. Minimum Necessary standard does not apply to:
 - 1. disclosures to a health care provider (doctor, hospital therapist etc.) for treatment purposes
 - 2. disclosure to the individual
 - 3. disclosure authorized by the individual
 - 4. disclosure to Department of Health and Human Services
 - 5. disclosure or use required by law
- F. Application of rule by County Employee
 - 1. Use only what you need to do your job
 - 2. Ask for only what you need
 - 3. Disclose only what the requester needs

VII PERMITTED DISCLOSURES OF PHI

- A. To a health care provider for treatment – minimum necessary does not apply
- B. To obtain payment – Auditor, Medicaid, Medicare and Health Insurers – minimum necessary
 - 1. Can rely on the payor as to what is minimum necessary
- C. Health Care Operations – mostly oversight and professional review issues Maplewood, Mental Health and Nursing Service
- D. Authorization –
 - 1. limited to the terms of the authorization – the person to whom and the PHI disclosed
 - 2. e.g. to the individual’s lawyer
- E. To Public Health Authorities – minimum necessary
 - 1. may rely on the Authority for minimum necessary
 - 2. except where required by law – minimum doesn’t apply
- F. To report known or suspected child abuse/neglect to appropriate authority
- G. To a business associate – minimum necessary applies
 - 1. requires a business associate agreement by April 14, 2004 or next contract whichever sooner

2. each Department's HIPAA Compliance Officer should maintain Business Associate contracts
 3. where Business Associate is another County Department, Memorandum of Understanding
 4. Business Associate agrees to use and disclose PHI we give it in accordance with HIPAA.
- H. To the Individual's Legal Representative
1. e.g. Executor of deceased individual, Guardian of an Incompetent, Health Care Proxy (not Power of Authority unless specific), parent or legal guardian of minor

VIII INCIDENTAL DISCLOSURES

A. Conversations – Rule recognizes that inadvertent disclosure can occur from oral transmissions e.g. treatment settings

1. O.K. as long as reasonable precautions are taken:
 - a. lower voices
 - b. move locale of discussion
 - c. barriers, cubicles, dividers, curtains

B. Offices – Computer screens, hard copies

1. locate screens out of direct sight of others
2. put info away when dealing with public, unauthorized employees
3. lock files and lock unoccupied offices

C. Leaving messages on answering machines

1. limit information
2. honor requests for specific arrangements

D. Sign in sheets and calling out names in waiting room

E. Patient charts – o.k. – face info away from passersby

F. Don't have to document incidental disclosures

IX NON RECURRENT DISCLOSURES

A. Recurrent are usual disclosures you do in performing your duties on a day to day basis

B. Non-Recurrent pursuant to requests from someone for their purposes

C. Required by Law

1. Must be a specific mandate that compels you to disclose
 - a. court order
 - b. subpoena from grand jury
 - c. court summons or court's subpoena
 - d. administrative subpoena
 - e. statute – medicaid or medicare
2. Identify the person or agency requesting – obtain authority or basis for request
letterhead, card o.k. for identification
3. Disclosure should be limited to the specific PHI required by the mandate
4. Make record of disclosure and give to Coordinator

D. Public Authority – authorized by law to obtain

1. Public Health Authority – Health Dept., Public Nurses, FDA
2. Child Abuse/Neglect – mandated report
3. Adult Abuse/Neglect, Domestic Violence
 - a. to social services e.g. or law enforcement
 - b. if individual agrees, or

- c. if disclosure is authorized by law and
 - c1. You believe it is necessary to prevent serious harm to the individual or other victims; or
 - c2. The individual is incapacitated and law enforcement represents that PHI is not intended to be used against the individual and an immediate law enforcement activity will be naturally and adversely affected by waiting for capacity of individual
- d. must inform the individual of this disclosure except if
 - d1. informing him would place him in risk of serious harm
 - d2. you would be informing a personal representative who you believe is responsible

E. Judicial and Administrative Proceedings, Subpoenas and other Discovery or Process – Must obtain satisfactory assurance

- 1. That individual has been given notice of the request; or
- 2. that reasonable efforts have been made to obtain a qualified protective order; or
- 3. that reasonable efforts have been made to give notice to the individual; or
- 4. that the individual has had sufficient time to raise an objection to the tribunal, and the time has elapsed without objection or the objections have been overruled; or
- 5. You notify the individual and give him sufficient time to object

F. Law Enforcement Requests can be honored:

- 1. for the purpose of identifying or locating a suspect, fugitive, material witness or missing person – only the following information: Name, address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death (if applicable) description including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos
 - but not:** individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.
- 2. to alert law enforcement of the death of a person believed to have died as a result of criminal conduct.
- 3. the PHI evidences criminal conduct on the premises
- 4. in medical emergency, to alert of the commission of a crime, the location of a crime, the location of the perpetrator
- 5. to a coroner to identify the person and determine cause of death etc.

G. Research purposes

H. Threat to health or safety

- 1. if it is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public
 - 1a. must be made to a person able to prevent or lessen the threat or
- 2. is necessary for law enforcement authorities to identify or apprehend an individual
 - 1a. because of a statement by an individual admitting participation in a violent crime that may have caused serious physical injury to the victim or
 - 1b. where it appears the individual is an escapee from custody
- 3. to a correctional facility if necessary for the health and safety of the individual, other inmates, employees of the facility, or for law enforcement or the administration of safety, security and good order

I. These matters should be handled by the Compliance Coordinator, with the assistance of the County Attorney's Office

X ADMINISTRATION OF INDIVIDUAL RIGHTS

A. Employees Duty

1. Documentation – forms supplied
2. Referral to Compliance Coordinator

B. RIGHTS

1. To request restriction of uses and disclosures
 - a. Department does not have to agree to comply to request
2. Alternative means or locations for communication with individual - must comply if reasonable
3. To request access to one's PHI – except for
 - a. psychotherapy notes
 - b. PHI compiled in a civil, criminal or administrative action
 - c. PHI obtained from another entity under a promise of confidentiality
 - d. a licensed health care professional determines it reasonably likely to endanger the life or physical safety of someone
 - e. the PHI refers to another person and health care professional determines that access will cause substantial harm to that person
 - f. a personal representative has requested the PHI and a health care professional has determined that access by the representative is likely to cause substantial harm to the individual or another person
4. To amend the individual's PHI
 - a. may deny if:
 - i. PHI is accurate and complete
 - ii. PHI is created by another entity
 - iii. PHI would not be available for access under above
 - b. 60 days to comply
 - c. must notify others to whom you have disclosed the PHI you amend
 - d. individual has a right to submit a written disagreement with the denial to be placed with the PHI
5. To obtain an accounting of disclosures
 - a. does not pertain to recurring disclosures
 - b. does not pertain to permitted disclosures
6. To complain about alleged violations or wrongful denials
 - a. to HIPAA Compliance Administrative through HIPAA Coordinator
 - b. to Department of Health and Human Services

Saratoga County Public Health

THE FAMILY EDUCATIONAL RIGHTS TO PRIVACY ACT (FERPA)

FERPA DESCRIBES HOW EDUCATIONAL INFORMATION ABOUT A STUDENT MAY BE USED AND DISCLOSED AND HOW THE STUDENT CAN GET ACCESS TO THIS INFORMATION.

Please read and familiarize yourself with your protections under FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Saratoga County Public Health is required by The Family Educational Rights to Privacy Act (FERPA) to maintain the privacy of the student's personally identifiable educational information (PIEI) and annually to give you this notice of legal duties and privacy practices with respect to educational information. This notice may be revised at any time and any revisions of this notice will be effective for past, present or future PIEI contained in the Agency's record.

Your Rights under FERPA:

- You have a right to inspect or review your child's early intervention/preschool education record (PIEI) when a written request to the originator of that portion of the PIEI that you want (the person or agency who created the document). If you are unable to submit a written request, a verbal request will be honored. The originator of the document will provide an explanation or interpretation of the information upon request. If your child is receiving Early Intervention Services, your service coordinator will assist you in making the request. If your request to access is approved and you request a copy of these records, the Agency can charge a fee of up to 10 cents per page (25 cents for second copy) of Early Intervention Program Records and up to 75 cents per page of Preschool Education Program Records, (NYS allowed rate) The fee will be waived if it prevents the parent (PIEI) from exercising their rights to access. The copy will be provided to you within 10 working days, unless the request is made as part of mediation or an impartial hearing, when the chart will be made available within 5 working days.
- You may request an amendment to PIEI. A written request must be received by the originator of PIEI stating that portion of the education record you wish amended, and must include the reason for your amendment request. Your request will be reviewed, but your request for an amendment may be denied. You have a right to a fair hearing if you are denied an amendment. The record will contain a statement to be kept and disclosed with the record if the record is not amended as the result of a hearing.
- You have a right to lodge a complaint in writing with the Early Intervention Official if you feel your FERPA rights are violated. Written complaints can also be made directly to the Office of Compliance at the following address: Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue, S.W., Washington, DC 20202-4605.
- The Agency does not disclose (PIEI) directory information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. If in the future the Agency begins to provide directory information, you will be given notice by the Agency of its change in practice, notified of what is included in the contents of the directory, provided with a specific timeframe to submit a written refusal to allow the Agency to disclose (PIEI) as directory information. Former (PIEI) may be disclosed as part of directory information without meeting the conditions stated above.

Saratoga County Public Health

- The Agency does not disclose the final results of a disciplinary proceeding conducted by an institution when a victim of a crime of violence or a non-forcible sex offense is involved with respect to that alleged crime or offense.

Disclose with your consent:

Written permission is required for examples not covered by this notice or applicable law. Your consent to disclose or to re-disclose PIEI to other parties must be obtained, except to the extent that NYS and Federal Laws authorize disclosure without consent. Written parental consent includes the names of both entities involved in releasing and obtaining of information, which records will be obtained or released, the specific record to be used and the purpose of such use; the date the parent signed the consent and the parent's signature and relationship to the child. When parental consent is obtained to disclose personally identifiable information, only information appropriate or specific to a request is released.

Disclose without your consent:

- To institutions or parties who have a legitimate educational interest.
- To school officials with a legitimate interest or to another educational institution where the (PIEI) seeks or intends to enroll, or when the disclosure is initiated by the parent or eligible (PIEI)
- To authorized representatives of the: Comptroller General or Attorney General or Secretary of the United States, or State and local educational authorities.
- To organizations conducting certain studies for, or on behalf of, educational institutions are permitted only if the study requests PIEI of parents and students.
- To accrediting organizations to carry out their functions.
- To parents of a dependent student.
- The Agency or the parent initiates legal action against either party, and those records relevant to the action are provided to the court, without an order.
- In an emergency, if the knowledge of the information is necessary to protect the health or safety of the student or other individuals.
- When specifically authorized by law, or
- When disclosure is required to Officials of the Federal and/or State Government is required in connection with audit/evaluation, or
- When enforcement of or compliance with Federal legal requirements related to educational programs is being evaluated.
- To comply with a judicial order or lawfully issued subpoena.
- The Agency will make a reasonable effort to try to contact you to notify you of receipt of an order or subpoena, unless we are specifically ordered by law not to.

Complaints:

Submit to the Agency's Early Intervention Official at: Phone # 518-584-7460

Karen A. Levison, Public Health Director/Early Intervention Official
Saratoga County Public Health Nursing Service
31 Woodlawn Avenue, Suite 1
Saratoga Springs, New York 12866-2198

If you believe that the student's educational rights have been violated, you have the right to complain without fear of reprisal or retaliation.