Intermediate Level

SELF-LEARNING MODULE (SLM)

2012 HIPAA Education
Privacy Basics and Intermediate Modules

Privacy Module

Privacy 101 and Intermediate Privacy Self-Learning Module
2012 HIPAA Education

Index

Page	
2	Index
3	Instructions
4	Course Description and Objectives
5	Self-Learning Module Part I: Privacy 101
	Education Requirements
	Definitions
	Notice of Privacy Practices/What we tell our patients
6	Confidentiality Violations
7	Patient Directory and Disclosure to the Public and the Media
8	Standard Safeguards
	Proper Disposal
	Computer Security
9	Providing Privacy
	Reporting Responsibilities
10	Self-Learning Module Part II: Intermediate Privacy
	Health Care Responsibilities
	Health Information, Access, Use & Disclosure Policy
11	Use and Disclosure of PHI
12	Mandated or Permitted Disclosures
	Requests for Information
13	Patient Authorization
	Patient Privacy Rights
14	Patient Requests
15	Denying at Patient’s Request
	Patient Complaints
16	Faxing Information
17	Misdirected Faxes
	Our Responsibilities

Privacy 101 and Intermediate Privacy Self-Learning Module
2012 HIPAA Education

Instructions

1. Obtain the following Packets:
   a. Intermediate Level Privacy Module
   b. Supplemental forms:
      - DOs/DON'Ts Tip Sheet
      - Policy Education summaries
      - Confidentiality and Non-Disclosure Agreement
      - Post-test

2. Read the self-learning module objectives.

3. Read the self-learning module.

4. Sign the Confidentiality and Non-Disclosure Agreement

5. Complete the post-test

6. Turn both the signed agreement and the post-test in to your manager or supervisor.

IMPORTANT: Receipt of the signed agreement AND completed post-test are proof of your completion of this program. Please submit these documents no later than April 7, 2003.

Privacy 101 and Intermediate Self-Learning Module
2012 HIPAA Education

Description

Part I: Privacy 101 – The goal of this self-learning module is to provide you with an understanding of your roles and responsibilities under the key privacy policies. These include the Confidentiality of Health Information, The Notice of Privacy Practices, and the Guidance for the Disclosure of Patient Directory Information to the Public and the Media.

Part II: Intermediate Privacy – This privacy module is an overview of key policies that you need to know if you regularly access and/or disclose Protected Health Information (PHI) as part of your job responsibilities. Once completed, you will be able to identify your responsibilities for the protection of PHI, the rights patients have regarding their PHI, the categories of authorization for disclosure of PHI and safeguards to apply to fax transmissions.

Objectives

Part I: Privacy 101
At the completion of this program the participant will be able to:

1. Understand your role and responsibilities under Privacy policies:
   a. Confidentiality of Health Information
   b. Notice of Privacy Practices
   c. Health Information, Disclosure to Public, Patient Directory, and Media

Part II: Privacy 201 Intermediate
At the completion of this program the participant will be able to:

1. Identify three key responsibilities you have for the protection of health information.
2. Identify new patient rights under the HIPAA Privacy rule and corresponding policies.
3. Identify categories of authorization for disclosure of information.
4. Identify safeguards to apply to facsimile transmission of information

Welcome to HIPAA Privacy 101

Privacy Education Requirements: In keeping with privacy regulations under HIPAA (Health Insurance Portability and Accountability Act), our organization is required to educate its entire workforce on the privacy policies that are to be followed when doing your job.

Important Policy Terms

Privacy – An individual's right to control the use and disclosure of his/her health information.

Confidentiality – Our obligation to protect the privacy of records and related information for all patients, employees, physicians, volunteers, and others that receive our care and services. We are all charged with protecting the privacy and confidentiality of patients, employees, physicians, volunteers and others who receive our care and services.

PHI – Protected Health Information includes all information that identifies an individual: Patient Name, Contact Information, Social Security Number, Age, and Diagnosis are some examples. Any aspect of information that identifies an individual is considered confidential. This included information that relates to a past present or future medical condition, the actual provision of health care and past, present or further payments for health care.

PHI is more than the Medical Record. It also includes:

- Written communications
- Patient stamper plates
- Electronic forms
- Verbal conversations
- IV and medication labels
- X-rays, monitors, EKGs, etc

Think of all the places you might find PHI, other than in a patient's medical record: Memos, E-mails, post-its, electronic forms, X-Rays, and even your own conversations may include PHI.

Notice of Privacy Practices: This is our commitment to protect the privacy of our patient information. So that patients and their families fully understand our commitment to their privacy, beginning in April 2003 we will provide the Notice of Privacy Practices at registration.

What We Tell Our Patients

Beginning April 2003, we will be providing all of our patients with the Notice of Privacy Practices. It informs our patients of:

- ways we may use and disclose his/her PHI
- individual's rights
- our legal responsibilities

The Notice of Privacy Practices explains to Patients how we may use and disclose their protected health information, their individual rights regarding their health information and our legal responsibilities with respect to their health information. This notice is similar to something you probably have received from your bank or other financial institution.

All patients will be asked to confirm that they received the notice by signing a Notice of Privacy Practices Acknowledgement. The Notice is widely available to patients:

- In registration areas
- On the internet
- Posted in our service locations

We Commit to Confidentiality of Patient Information. A Confidentiality and Non-Disclosure Agreement is signed by all members of the workforce. The confidentiality policy applies to EVERYONE in the workforce and a Confidentiality and Non-Disclosure agreement must be signed by everyone, including physicians and volunteers.

Violations of Confidentiality are a Serious Matter: Violations of confidentiality will result in corrective action, which may include termination of employment and personal legal consequences.

Violations include:

- ➢ Failure to comply with privacy policies and procedures and federal regulations.
- ➢ Wrongful access, use and disclosure of protected health information
- ➢ Failure to safeguard patient's health information

THIS CAN BE SERIOUS BUSINESS!

Patient Trust Must Be Maintained. The most important consequence of violations is that we may lose our patients' trust.

<u>Confidentiality Violations</u>
Do not view, obtain, or share information about yourself, co-workers, family, friends or any patients unless authorized to do so. Of course, violations can be easily avoided. Just don't view, obtain, or share information about patients, co-workers, yourself, or even your family or friends unless you are authorized to do so.

<u>Patient Directory and Disclosure to Public & Media</u>
Disclosure of Information to the Public: The In-Patient Directory

- ➢ A directory of information about current hospitalized patients.
- ➢ On admission, patients are asked if they want their information included in the directory.

Each Hospital maintains a directory of information about current hospitalized patients. On admission, the directory is explained to patients, and they are asked if they want their information included.

Directory Information

- ◆ Patient name
- ◆ Location (e.g. in-patient, Emergency Dept.)

- Condition-one word (e.g. good, fair, serious, critical)
- Religion (available <u>only</u> to clergy)

Patients who agree will have this information and a one-word condition (such as fair, good, serious, or critical) listed in the directory. With the exception of religion (which can only be disclosed to clergy) this information can be disclosed to members of the public and the media who ask for the patient by name.

Disclosing Directory Information

- An individual must ask for the patient <u>by name</u>.
- Only the location and general condition of the patient is provided
- Patients requesting not to be in the directory are confidential and will not appear in Information Desk Screen.

When a patient can not be found in the directory, inquiries are answered with, “We do not have that name in our hospital directory.” If a caller is persistent, as supervisor or media relations staff member is contacted for assistance.

<u>Exclusions from Directory</u>

Certain patient populations, such as Behavioral Health patients are never included in the directory to further protect their confidentiality.
No information on these patients is ever released.

<u>Requests for Information in Outpatient/Clinic Areas</u>

- Basic patient appointment information may be released to individuals who are involved in the patient’s care.
- Refer calls to a nurse or supervisor if unsure of caller’s request for information.

<u>Patient Requests</u>

- Patients may have special requests for communicating or limiting disclosure of their information.
- Notify your supervisor to speak with the patient about their request

We will always do our best to accommodate reasonable requests.

<u>Requests for Information from the Media</u>

- Refer media requests to a Communications representative or supervisor.
- Provide only unrestricted patient directory information.
- Patients must approve Media visits. Coordinate with Communications.
- Media should be escorted while in the facility.

When a request comes from a media representative, the same directory guidelines should be followed. Additionally, media visits to patients <u>MUST</u> be coordinated through media relations/communications staff. Media representatives must ALWAYS be escorted while in the facility.

<u>Apply Standard Safeguards to Protected Health Information</u>

Important Safeguards:

- **Know your department’s specific privacy policies.**
- **Restrict patient information to those who have a “need to know.”**

- **Protect health information from unauthorized access.**
- **Never leave patient charts or computer screens open to the public view.**

ALWAYS protect patient health information from unauthorized access, use, or disclosure. Patient information is restricted to only those who have a need to know. Some departments have their own specific privacy policies. Make it a point to learn them and know them.

Confidential Conversations should be held in a private area whenever possible. Never hold conversation about patients in public areas (elevators, cafeteria). Confidential information should always be discussed in private.

Never Leave Medical Information Unattended: Unattended medical information can cause major problems. If you notice health information that is unattended, please notify clinical staff right away or take steps to secure it. Always use minimal information when in public view (e.g. white boards) so that patients cannot be identified.

Do not expose protected health information while transporting patients (e.g. having the label with patient name within view.

Limit Access to Authorized Individuals: Keep doors to secure areas closed. Make use of the safeguards we have in place. Keeping doors to secure areas closed can help prevent privacy violations.

Proper Disposal

Never dispose of paper or items containing patient information in the regular trash. Remember-PHI is not only paper! (Includes blue stamper plates too). Ask yourself, “Does this include patient information?” If the answer is yes, then it doesn’t go in the regular trash. **Dispose of PHI the right way – SHRED IT! When paper items include patient information, they should be disposed of in department shredding boxes. Non-paper items should be destroyed in other ways.**

Computer Security

- Never share your computer password with anyone or log on to a computer for someone else to use.
- Logout or use secure screensavers when leaving computer unattended.

A lot of privacy information can be found on the computers we use (including PYXIS). Never share your password with anyone and never log on to a computer for someone else to use. Screen savers can also be of help when you leave a computer unattended.

Provide Privacy
When discussing private medical information with patients or their families, find a private area for your discussion.

Avoid Public Areas
Never discuss confidential information in public areas, such as hallways, cafeterias, elevators, & restrooms.

Question Strangers in Your Work Area: If you see someone in your work area that doesn't look familiar, question them. Find out if they belong there.

Before leaving at the end of your shift: Empty Your Pockets: Never remove patient information from the facility. Never take patient information home or leave it in a locker or unsecured place.

Reporting Responsibilities

Everyone is responsible for reporting known or suspected instances of unauthorized access, use or disclosure of protected health information. If you see or hear something you suspect is a violation of the confidentiality policy, you should report it. We all have responsibility for protecting health information.

Reporting Leads to Improvement of Our Privacy Practices. Report **Suspected** Violations or Concerns. There will be no retaliation against individuals for reporting suspected privacy violations in good faith. The important thing is to report your concerns so the problem can be corrected as soon as possible.

Reporting Options:

- Report to Supervisor, Manager, or Department Head
- Occurrence Report
- Privacy Team Leader
- Patient Relations
- Human Resources
- Privacy Officer
- Compliance

Choose the one that works best for you and will solve the problem in the quickest amount of time.

In Summary

- ✓ Access only information needed to do your job.
- ✓ Report suspected privacy violations.
- ✓ Treat protected health information (PHI) as if it were your own.

Part II: Intermediate Privacy
For Workforce Handling Protected Health Information

Our Obligation to the Patient: Our Responsibilities

- To effectively manage and <u>safeguard</u> their personal health information
- Establish policies and best practices for the management of PHI
- Support and encourage the patient's right regarding their PHI

We understand that information about our patients and their health is confidential. Our responsibility is to effectively manage and <u>safeguard</u> their PHI. In order to fulfill our obligations to the patient, we have developed policies that establish best practice for the management of PHI and support and encourage the patient's rights regarding their PHI.

Notice of Privacy Practices

- Serves as the main communication to patients
- Educates patients on:
  - their rights
  - our responsibilities for protecting their PHI
  - how we may use and disclose their PHI
- Directs patients where to go for questions and concerns regarding their PHI

3**Beginning April 14, 2003, we must provide every patient with a copy of our "Notice of Privacy Practices"**.

Notice of Privacy Practices

- Patients are provided Notice at their first service/registration encounter
- Patients sign an acknowledgement that they received the Notice
- Acknowledgement of receipt is documented on the registration screen

<u>Health Information, Access Use & Disclosure Policy</u>
"Access Control"

- Access to PHI is based on "need to know" and "minimum necessary" principles
- Individuals needing access to PHI are those:
  - ✓ providing care and treatment
  - ✓ performing payment/billing activities
  - ✓ participating in of healthcare operations

The general guiding principle is that access to protected health information is always based on "need to know." Only the "minimum necessary" PHI should be used or disclosed for the purpose at hand. Individuals recognized as needing to have access to PHI are those who provide care and treatment, perform payment or billing activities or who participate in functions of healthcare operations.

“Use” of PHI
A “**use”** of PHI occurs with information gathered while providing patient care within the organization, and is kept under our direct control. Examples include:

- A nurse in a clinical care setting may “use” Protected Health Information when giving a “report” to the oncoming nurse.
- A Case Manager may “use” information to review patient stays.

“Disclosure” of PHI:
“Disclosure” of information occurs when information is communicated or transmitted outside of the organization. This may be to another individual or facility or the entry of data into an electronic communication mechanism such as claim submission.

TPO: **T**reatment, **P**ayment, Healthcare **O**perations
The organization is generally permitted to use and disclose Protected Health Information without specific patient authorization when providing treatment, obtaining payment or conducting healthcare operations. Obtaining Payment includes communicating a patient’s health information to obtain payment for services or treatment by electronic or other means. This may also include disclosure of PHI to obtain pre-authorization for treatment and procedures from the patient’s insurance plan, or retrospective review of the patient’s medical record by the payer.

Processes that fall under the category of Health Care Operations include sharing a patient’s health information as necessary to operate our healthcare facility and for quality processes – and sharing a patient’s health information with other healthcare providers who have had a relationship with the patient. Examples of quality-related activities include post-discharge telephone calls to follow-up on the patients health status, granting medical staff credentials to physicians, administrative activities involving financial and business planning and development, customer service activities and investigation of complaints.

There are some exceptions to TPO that do require specific patient authorization. Certain categories of PHI are considered highly confidential and are therefore further protected by Federal and State law. Disclosure of information in these categories requires a specific authorization from the patient. These include records related to drug and alcohol abuse treatment, HIV and AIDS test results and mental or behavioral health.

All PHI being disclosed should be screened for the presence of this type of information. Obtain the patient’s authorization for this specific information to be released. Contact the Health Information Department if you have questions.

Disclosures that are Mandated or Permitted
Certain disclosures are mandated or permitted by State and Federal law or certain government agencies. These types of disclosures do not require a patient authorization. State and Federal law and certain government agencies mandate reporting or permit disclosing of PHI by healthcare providers. These types of disclosures do not require a patient authorization.

Examples of Disclosures that are Mandated or Permitted:

- Organ and tissue donation
- Public health activities
- Health oversight agencies
- Coroners, Medical examiners and mortuaries
- Military Commands
- Workers Compensation
- Correctional Facilities
- Law Enforcement
- Serious threat to health or safety

Permitted Disclosures to Law Enforcement

- Responding to a court order, subpoena, or similar process
- Identifying or locating a suspect, witness or missing person
- Reporting about crime victims

Certain circumstances allow the disclosure of information to law enforcement. Each circumstance of disclosure to law enforcement has limitations as to the elements of information that are permitted to be disclosed. We have developed a specific policy on Disclosure of Information to Law Enforcement for additional guidance. Key points are to release the minimum amount of information necessary to respond to the law enforcement request (whether verbal or written) and to refer all written requests for information to the Health Information Department.

All permitted and Mandated Disclosures must be documented. These are disclosures that the patient would not necessarily know had been made and must be listed if the patient requests an accounting of disclosures of their PHI. Options for documentation include: recording the disclosure in the clinical record, or on a mandated reporting form or, by completing a " PHI Disclosure Documentation" form, which is forwarded to Health Information for inclusion in the medical record.

Requests for Information

Respond to requests when necessary to ensure patient safety, treatment, and continuity of care. In the absence of Health Information personnel, a supervisor, charge nurse or designee may respond to requests when necessary to ensure patient safety, treatment, and continuity of care.

When friends and family ask for information: Clinical staff may disclose information to family or friends directly involved in the patient's care. Patients identify the individuals directly involved in their care who may be provided information.

Handling Requests for Information

There are critical steps when responding to requests for PHI that include validation of the identity and authority of the person requesting the information and documentation.

✓ For in-person requests, check a photo ID.
✓ For phone requests, identity may be validated by call back to the requestor.
✓ Be sure to document the validation method used and the information disclosed.

Disclosures Requiring the Patient's Authorization

- Research

- Marketing
- Fundraising

Generally disclosures requested outside of TPO or mandated or permitted disclosures, require a patient authorization. Authorizations are required in order to disclose health information involving a research study. Authorizations are required for marketing activities except for direct face to face communications or when giving gifts that are of nominal value. Authorizations for fundraising activities that use more than demographic or dates of service information.

Patient Authorization

An Authorization for Use or Disclosure Form must be completed.
Important: If any of the required elements are not completed on the authorization, the authorization is INVALID and we may not act on the request!

We require completion of a standard authorization form for use or disclosure of patient's PHI. This form -"Authorization for Use of Disclosure of Health Information" - is available in all clinical areas, or is available from the Health Information Department.

In order for a patient authorization to be valid, all elements on the form must be completed with the patient's signature or that of his legal representative.

In Summary: *for Access, Use and Disclosure of Information...* Our Work Force is responsible for appropriate disclosure of information in compliance with laws and regulations, patients' rights, and with what is in the best interest of the patient. If you have a question about the type of authorization needed for a disclosure, consult your supervisor, the Heath Information Department or Legal Department for assistance.

Patients Privacy Rights

Patients have a right to:

- Request restrictions on use and disclosure of their information.
- Request amendments to their Health Information
- Request an Accounting of Disclosures
- Inspect and copy their information
- Complain about our Information Practices

The Privacy Regulations ensure that our patients have certain rights regarding their PHI. Policies have been developed in these key areas to ensure that our patients may exercise these rights.

Our patients may request restrictions on the use and disclosure of their PHI. Patients must make these requests in writing. Each request will be evaluated on an individual basis. Refer requests to the health Information department or your supervisor. We will accommodate requests based on our information system capabilities to restrict the information.

Patient Requests For Alternative Communication

Patients may request that communications about their PHI be made in a certain way or a to a certain location. For example, a patient may request that a bill be sent to an alternate address. Our staff will work with patients to accommodate reasonable requests.

Patient Requests to Amend their Health Record:
Patients must submit the request in writing to the Health Information Department. Patients may request an amendment to health information in their medical record if they believe the information is inaccurate or incomplete. Patients submit the request for amendment in writing to the Health Information Department.

Patient Requests for Accounting of Disclosures
Patients may request an accounting of certain disclosures of their PHI made outside of the organization. Patients have a right to obtain an accounting of certain disclosures of their information that have been made outside of the organization.   This accounting would include disclosures that the patient may not be aware of. We do not have to account for disclosures made for treatment, payment or healthcare operations (TPO) or disclosures authorized by the patient. Requests by a patient for an accounting of their disclosures are handled by the Health Information Department.

Disclosures That Must Be Accounted For

Examples include:

- Disclosures to Law Enforcement
- Abuse, assault, neglect
- Judicial and administrative proceedings
- Public health activities
- Organ and tissue donation
- Data collection preparatory to research

Many of the disclosures that must be accounted for fall under the category of mandated and permitted disclosures. In many cases, the patient may not be aware of these disclosures.

Patient Requests to Inspect or Obtain a Copy of their PHI
When a patient requests a copy of their record for inspection and /or copying, the request must be in writing and directed to the Health Information Department at the place where treatment was provided. Provide the patient with the “Authorization for Use and Disclosure of Health Information” form. Forward the original signed form to the Health Information Department and provide a copy to the patient. The Health Information Department is responsible for providing information and copies of information to the patient upon request.

Patient Requests in Outpatient Departments
Copies of Individual PHI (i.e. lab results, x-ray films) provided to a patient at the request of their physician must be documented.

- Have patient complete an “Authorization for Use and Disclosure of Health Information” **or** document in the medical record specifically what the patient was provided.

- File the release into the chart **or** forward to the Health Information Department for inclusion in the chart.

When you provide these complete the “Authorization of Release Form “ or document the information provided in the clinical record. This ensures that there is documentation of what was given to the patient, should the records end up somewhere publicly.

Patients Requests To View Their Health Information
If patients request to view their current health information, inform them that the open medical record is incomplete and, for that reason, an authorization from their physician is necessary. Obtain an order from the patient’s (attending) physician and ensure that an appropriate clinical person is assigned to accompany the patient during review.

Denying a Patients’ Request to View Their Health Information
Be aware, there are instances in which patient access may be denied. Consult with Health Information or an Operations Supervisor. Examples include information that is:

- Obtained in the course of research that includes treatment that may be temporarily suspended
- Obtained through a third party under a promise of confidentiality
- Denied per direction of a correctional institution
- Determined by a licensed professional as reasonably likely to endanger the individual or others

Patient Complaints
Patient complaints or concerns regarding our information practices should be addressed through existing channels:

- Patient Relations/ Risk Managers
- Privacy Team Leader
- Privacy Officer
- Compliance phone line

Patients may also file a written complaint and request an investigation to the Department of Health and Human Services. The Notice of Privacy Practices includes specific information regarding how our patients may complain to the organization OR to the Secretary of the Department of Health and Human Services. In addition, the notice informs patients that no one will be retaliated against for filing a complaint. The notice also contains contact information for the Privacy Officer. All written complaints should be directed to the Privacy Officer.

Privacy Consideration: Faxing of Information

A key privacy policy is Facsimile of Information. This policy provides guidance for the appropriate facsimile transmission and receipt of health information.

When Is Faxing Appropriate? Consider faxing when:

- Needed urgently for patient care or to obtain payment
- Authorized by the patient/legal representative

Consider faxing PHI when the original record or mailing delivered copies will not meet the immediate needs of patient care, or when information is urgently required by a third party payor in order to secure reimbursement, or has been specifically authorized by the patient or his/her legal representative. Always consider security of information, be alert, and decide when faxing may not be the best method of delivering PHI.

Faxing PHI

When a fax contains protected health information, first determine if specific or additional authorization is required.

- ✓ Ask yourself, “Is the information necessary in order to facilitate patient safety, treatment, healthcare operations or continuity of care?”
- ✓ Verify that the recipient has the authority to receive the information.
- ✓ Never fax more than the minimum amount of information necessary to facilitate patient safety, treatment, healthcare operations and continuity of care.

Apply Faxing “Best Practice”

- Verify the accuracy of fax numbers before sending
- Pre-program frequently called numbers to cut down on dialing errors; send a test fax and verify receipt
- Notify others if your fax number changes

…and Faxing Safeguards…Ensure your fax machine is in a secure location. Do not place your fax machine where it is accessible to the public. Do not let faxes sit on the machine for extended periods of time; provide a means of sorting incoming faxes until they can be picked up. Do not read fax communications that are not intended for you.

Use a Fax Cover Sheet!

- Cover sheets are required for all transmissions

The fax cover sheet template is available for your use. ” In general facsimile Cover sheets are required for all transmissions. We have developed a standard Confidentiality Statement to be included in all organizational fax cover sheets.

If patient medical records are being faxed, include the standard Disclaimer/Warning developed by the organization.

Exception to Fax Cover Sheet

All of the following must apply:

- ✓ destination is within the facility
- ✓ destination fax number is preprogrammed
- ✓ receiving fax machine is in a controlled access area

A Misdirected fax containing PHI is considered a disclosure of information and may present significant risk. If this happens, do the following:

- Immediately transmit a request to the unintended receiver requesting that the material be destroyed immediately or returned by mail. Save documentation of this transmission.
- Obtain the correct fax number of the intended recipient and re-transmit.
- Misdirected Faxes Containing PHI
    - Complete an Occurrence Report
    - Follow facility procedures

Our Responsibilities

Protecting and managing health information is complex. It takes all of us doing our part and upholding our responsibilities to:

- Control access to protected health information
- Use and disclose only the information necessary to meet the need
- Obtain authorizations for disclosures

Remember, privacy policies and procedures are designed to facilitate patients' control of their health information; facilitate the patients' ability to maximize their rights; and provide guidance for you to exercise best privacy practices in the management of protected health information.

If you have any questions regarding policies on privacy and confidentiality, you can discuss them further with your facility's Privacy Team Leader, you Manager or Supervisor, or the Privacy Officer.

ALL MEMBERS OF THE WORKFORCE PLAY A VITAL ROLE IN PROTECTING OUR PATIENTS' PRIVACY.