HIPAA INFORMATION

The Health Insurance Portability and Accountability Act (HIPAA)

Statement of HIPAA Portability Rights

Pre-existing condition certification no longer needed

Under HIPAA, you and your family members cannot be denied eligibility or benefits based on certain health factors, including pre-existing conditions, when enrolling in a health plan. In addition, you may not be charged more than similarly situated individuals based on any health factors.

The pre-PPACA requirement for HIPAA certifications on pre-existing condition or certificates of creditable coverage are no longer required.

Right to get special enrollment in another plan

Under HIPAA, if you lose your group health plan coverage, you may be able to get into another group health plan for which you are eligible (such as a spouse's plan), even if the plan generally does not accept late enrollees, if you request enrollment within 30 days. (Additional special enrollment rights are triggered by marriage, birth, adoption, and placement for adoption and may have longer enrollment periods.)

Therefore, once your coverage ends, if you are eligible for coverage in another plan (such as a spouse's plan), you should request special enrollment as soon as possible.

Prohibition against discrimination based on a health factor

Under HIPAA, a group health plan may not exclude you (or your dependents) from the plan based on anything related to your health. Also, a group health plan may not charge you (or your dependents) more for coverage, based on health, than the amount charged a similarly situated individual.

Special Enrollment Rights

Special enrollment allows individuals who previously declined health coverage to enroll for coverage outside of a plan's open enrollment period. There are two types of special enrollment:

Loss of eligibility for other coverage — Employees and dependents who decline coverage due to other health coverage and then lose eligibility or employer contributions have special enrollment rights. For example, an employee who turns down health benefits for herself and her family because the family already has coverage through her spouse's plan can request special enrollment for her family in her own company's plan.

Certain life events — Employees, spouses, and new dependents are permitted to special enroll because of marriage, birth, adoption, or placement for adoption.

For both types, the employee must request enrollment within 30 days of the loss of coverage or life event triggering the special enrollment.

State flexibility

This certificate describes minimum HIPAA protections under federal law. States may require insurers and HMOs to provide additional protections to individuals in that state.

For more information

If you have questions about your HIPAA rights, please contact your benefit plan administrator and/or the individual listed below:

_____
[HIPAA Compliance Officer or Plan Administrator]

at _____
Phone Number

HIPAA and the Definition of Spouse and Family

Following a Supreme Court decision in 2015 that legalized same-sex marriage, sections of HIPAA needed to be modified and expanded to incorporate the new definitions of spouse and family. Pursuant to the decision in *United States v. Windsor*, the term spouse now includes individuals who are in a legally valid same-sex marriage. The term marriage includes both same-sex and opposite-sex marriages, and family member includes dependents of either type of marriage.

These new definitions are relevant to the HIPAA Privacy Rule itself, to the HIPAA section concerning permission of covered entities to share protected health information (PHI) with family members, to the section concerning the Use and Disclosure of Genetic Information for Underwriting Purposes, and to other sections where spouse or family member is mentioned.

In 2016, the Department of Health and Human Services (HHS) issued a final rule on "Nondiscrimination in Health Programs and Activities" to expand discrimination protections under the Affordable Care Act and HIPAA. Individuals are now protected against discrimination in health care based on:

- Race • Color • National Origin • Age
- Disability • Sex and Gender Identity

HIPAA Privacy Rule

How It Came About

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information*, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.

The HIPAA Privacy Rule, in effect since 2003, establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The rule applies to Covered Entities and their business associates (subcontractors, providers and the like).

What the Rule Does

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.
- For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.
- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

What Information Is Protected

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow these laws

Covered Entities

Under the HIPAA Privacy Rule, Covered Entities and their business associates must guard against the misuse of an individual's identifiable health information and limit the sharing of such information.

Covered Entities include, but are not limited to, the following:

- Health Care Provider (hospitals, doctors, dentists, psychologists, clinics, pharmacies, nursing homes, and laboratories)
- Health Plans (eg. health insurance or self-insured) Dental Plans (eg health insurance or self-insured) Vision Providers (eg health insurance or self-insured)
- Employee Assistance Plans that provide health benefits (eg health insurance or self-insured)
- Health insurance providers
- PPOs, HMOs, and managed health care organizations
- Health Care Spending or Reimbursement Accounts (flexible spending accounts under a cafeteria plan)
- Medical billing services
- Health Care Clearinghouses

Who Is Not Required to Follow the Rule

Examples of organizations that do not have to follow the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

Your Rights Over Your Health Information

Health insurers and providers who are covered entities must comply with your right to:

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can:
- File a complaint with your provider or health insurer
- File a complaint with HHS

You should get to know these important rights, which help you protect your health information.

You can ask your provider or health insurer questions about your rights.

Who Can Look at and Receive Your Health Information

The Privacy Rule sets rules and limits on who can look at and receive your health information.

To make sure that your health information is protected in a way that does not interfere with your health care, your information can be used and shared:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot:

- Give your information to your employer
- Use or share your information for marketing or advertising purposes or sell your information

Anti-Discrimination Notice

General

Under current law, a group health plan may not establish any rule for eligibility (including continued eligibility) of any individual to enroll for benefits under the terms of the plan that discriminates based on any health factor that relates to that individual or a dependent of that individual.

Health Factors

The term "health factor" means, in relation to an individual, any of the following health status-related factors:

- Health status;
- Medical condition (including both physical and mental illnesses);
- Claims experience;
- Receipt of health care;
- Medical history;
- Genetic information;
- Evidence of insurability (including conditions arising out of acts of domestic violence or out of participations in recreational activities);
- Disability

Eligibility Rules

Rules for eligibility include rules relating to any of the following:

- Enrollment;
- The effective date of coverage;
- Waiting (or affiliation) periods;
- Late and special enrollment;
- Eligibility for benefit packages;
- Benefits (including copayments and deductibles);
- Continued eligibility;
- Terminating coverage (including disenrollment) of any individual under the plan.

Nonconfinement and Actively-At-Work Provisions

A plan may not establish a rule for eligibility or set any individual's premium or contribution rate based on whether an individual is confined to a hospital or other health care institution or whether the individual is actively at work (including continuous employment).

Similarly Situated Individuals

Distinctions among groups of similarly situated individuals may not be based on a health factor. Group health plans may limit or exclude coverage or benefits if the restriction is applied uniformly to all similarly situated individuals and is not directed at any individual participants or beneficiaries based on a health factor.

Exceptions for Wellness Programs

Special rules and exceptions apply to wellness programs (programs designed to promote health or prevent disease) that provide benefit incentives.

Breach Notification

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) requires HIPAA-covered entities and business associates to follow specific rules relating to the discovery of a breach of protected health information. These rules require covered entities and business associates to do the following when a security breach is discovered:

- Provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information.
- Provide notice to prominent local media outlets if there is a breach affecting more than 500 residents of a state or jurisdiction.
- In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach.

A "breach" is defined as the acquisition, access, use, or disclosure of protected health information in an impermissible manner which compromises its security or privacy.

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

The covered entity must send the required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered.

Mental Health

Information for the NICS

On January 4, 2016, the Department of Health and Human Services (HHS) modified the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a firearm.

The final rule gives states improved flexibility to ensure accurate but limited information is reported to the NICS. This rulemaking makes clear that, under the Privacy Rule, certain covered entities are permitted to disclose limited information to the NICS. The information that can be disclosed is the minimum necessary identifying information about individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs.

An individual who seeks help for mental health problems or receives mental health treatment is not automatically legally prohibited from having a firearm; nothing in this final rule changes that.

Protected Health Information (PHI)

What is Protected Health Information (PHI)?

Under the HIPAA Privacy Rule, protected health information, or "PHI," refers to individually identifiable health information that is created, received, stored, or transmitted in any form or medium by a covered entity or their business associate in relation to the provision of healthcare, healthcare operations and payment for healthcare services. Individually identifiable health information is that which can be linked to a particular person. Specifically, this information can relate to:

- The individual's past, present or future physical or mental health or condition;
- The provision of health care to the individual; or,
- The past, present, or future payment for the provision of health care to the individual; or
- The individual's genetic information.

PHI includes 18 identifiers that can be used to identify a patient, including:

- Name
- Address (including subdivisions smaller than state such as street address, city, county, or zip code)
- Any dates (except years) that are directly related to an individual, including birthday, date of admission or discharge, date of death, or the exact age of individuals older than 89
- Telephone and fax numbers
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers, serial numbers, or license plate numbers
- Device identifiers or serial numbers
- IP address and Web URLs
- Biometric identifiers such as fingerprints or voice prints
- Full face photos
- Any other unique identifying numbers, characteristics, or codes

What is Electronic Protected Health Information (ePHI)?

"Electronic Protected Health Information" or "ePHI" means Protected Health Information that is maintained in or transmitted by electronic media.

Uses & Disclosures of PHI

Covered entities must safeguard PHI by implementing policies and procedures to restrict access to and use of PHI. Furthermore, a covered entity must only use or disclose the minimum amount of PHI necessary.

Required disclosures include:

- To an individual when requested & required by Section 164.524 (Access) & Section 164.528 (Accounting)
- To HHS, to investigate or determine compliance with Privacy Rule
- To the FBI and the National Instant Criminal Background Check System (NICS) for mental health issues regarding gun possession

Besides required disclosures, covered entities also may disclose PHI to their patients / health plan enrollees so that:

- Health plans can contact their enrollees, and
- Providers can talk to their patients

Permitted Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) provided to the individual (unless required for access or accounting of disclosures); (2) used for treatment, payment, and health care operations; (3) granting opportunity to agree or object; (4) as an incident to an otherwise permitted use and disclosure; (5) for public interest and benefit activities; and (6) as a limited data set for the purposes of research, public health or health care operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

HIPAA Security Rule

What Is It?

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information.

HIPAA called on the Secretary to issue security regulations regarding measures for protecting the integrity, confidentiality, and availability of e-PHI that is held or transmitted by covered entities. HHS developed a proposed rule and released it for public comment on August 12, 1998. The final regulation, the Security Rule, was published February 20, 2003.

Who's Covered by the Security Rule?

The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates. The HITECH Act of 2009 expanded the responsibilities of business associates under the HIPAA Security Rule. Any telehealth provider's also need to meet HIPAA Security Rule regulations.

What Information Is Protected?

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

General Rules

The Security Rule requires covered entities and their business associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also provides the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.

HIPAA Privacy Rule

How It Came About

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.

The HIPAA Privacy Rule, in effect since 2001, establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.

The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The rule applies to Covered Entities and their business associates (subcontractors, providers and the like).

What the Rule Does

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.
- For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.
- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

What Information Is Protected

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow these laws

Who Is Not Required to Follow the Rule

Examples of organizations that do not have to follow the Privacy and Security Rules include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

Covered Entities

Under the HIPAA Privacy Rule, Covered Entities and their business associates must guard against the misuse of an individual's identifiable health information and limit the sharing of such information.

Covered Entities include, but are not limited to, the following:

- Health Care Provider (hospitals, doctors, dentists, psychologists, clinics, pharmacies, nursing homes, and laboratories)
- Health Plans (via health insurance or self-insurance) Dental Plans (via health insurance or self-insurance) Vision Providers (via health insurance or self-insurance)
- Employee Assistance Plans that provide health benefits (via health insurance or self-insurance)
- Health insurance providers
- PPOs, HMOs, and managed health care organizations
- Health Care Spending or Reimbursement Accounts (flexible spending accounts under a cafeteria plan)
- Medical billing services
- Health Care Clearinghouse

CONTINUED >>>

HIPAA Privacy Rule Continued

Your Rights Over Your Health Information

Health insurers and providers who are covered entities must comply with your right to:

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can
- File a complaint with your provider or health insurer
- File a complaint with HHS

You should get to know these important rights, which help you protect your health information.

You can ask your provider or health insurer questions about your rights.

Who Can Look at and Receive Your Health Information

The Privacy Rule sets rules and limits on who can look at and receive your health information.

To make sure that your health information is protected in a way that does not interfere with your health care, your information can be used and shared:

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot:

- Give your information to your employer
- Use or share your information for marketing or advertising purposes or sell your information

CONTINUED >>>

HIPAA and the Definition of Spouse and Family

Following a Supreme Court decision in 2015 that legalized same-sex marriage, sections of HIPAA needed to be modified and expanded to incorporate the new definitions of spouse and family. Pursuant to the decision in *United States v. Windsor,* the term spouse now includes individuals who are in a legally valid same-sex marriage. The term marriage includes both same-sex and opposite-sex marriages, and family member includes dependents of either type of marriage.

These new definitions are relevant to the HIPAA Privacy Rule itself; to the HIPAA section concerning permission of covered entities to share protected health information (PHI) with family members; to the section concerning the Use and Disclosure of Genetic Information for Underwriting Purposes; and to other sections where spouse or family member is mentioned.

In 2016, the Department of Health and Human Services (HHS) issued a final rule on "Nondiscrimination in Health Programs and Activities" to expand discrimination protections under the Affordable Care Act and HIPAA. Individuals are now protected against discrimination in health care based on:

- Race • Color • National Origin • Age
- Disability • Sex and Gender Identity

Statement of HIPAA Portability Rights

Pre-existing condition certification no longer needed

Under HIPAA, you and your family members cannot be denied eligibility or benefits based on certain health factors, including pre-existing conditions, when enrolling in a health plan. In addition, you may not be charged more than similarly situated individuals based on any health factors.

The pre-PPACA requirement for HIPAA certifications on pre-existing condition or certificates of creditable coverage are no longer required.

Right to get special enrollment in another plan

Under HIPAA, if you lose your group health plan coverage, you may be able to get into another group health plan for which you are eligible (such as a spouse's plan), even if the plan generally does not accept late enrollees, if you request enrollment within 30 days. (Additional special enrollment rights are triggered by marriage, birth, adoption, and placement for adoption and may have longer enrollment periods.)

Therefore, once your coverage ends, if you are eligible for coverage in another plan (such as a spouse's plan), you should request special enrollment as soon as possible.

Prohibition against discrimination based on a health factor

Under HIPAA, a group health plan may not exclude you (or your dependents) from the plan based on anything related to your health. Also, a group health plan may not charge you (or your dependents) more for coverage, based on health, than the amount charged a similarly situated individual.

Special Enrollment Rights

Special enrollment allows individuals who previously declined health coverage to enroll for coverage outside of a plan's open enrollment period. There are two types of special enrollment:

Loss of eligibility for other coverage — Employees and dependents who decline coverage due to other health coverage and then lose eligibility or employer contributions have special enrollment rights. For example, an employee who turns down health benefits for herself and her family because the family already has coverage through her spouse's plan can request special enrollment for her family in her own company's plan.

Certain life events — Employees, spouses, and new dependents are permitted to special enroll because of marriage, birth, adoption, or placement for adoption.

For both types, the employee must request enrollment within 30 days of the loss of coverage or life event triggering the special enrollment.

State flexibility

This certificate describes minimum HIPAA protections under federal law. States may require insurers and HMOs to provide additional protections to individuals in that state.

For more information

If you have questions about your HIPAA rights, please contact your benefit plan administrator and/or the individual listed below:

_____
(HIPAA Compliance Officer or Plan Administrator)

at _____
Phone Number

CONTINUED >>>

HIPAA Security Rule

What Is It?

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Secretary of HHS to publish national standards for the security of electronic protected health information (e-PHI), electronic exchange, and the privacy and security of health information.

HIPAA called on the Secretary to issue security regulations regarding measures for protecting the integrity, confidentiality, and availability of e-PHI that is held or transmitted by covered entities. HHS developed a proposed rule and released it for public comment on August 12, 1998. The final regulation, the Security Rule, was published February 20, 2003.

Who's Covered by the Security Rule?

The Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities") and to their business associates. The HITECH Act of 2009 expanded the responsibilities of business associates under the HIPAA Security Rule. Any telehealth providers also need to meet HIPAA Security Rule regulations.

What Information Is Protected?

The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information (PHI), as explained in the Privacy Rule. The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule calls this information "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

General Rules

The Security Rule requires covered entities and their business associates to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI. The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI. Under the Security Rule, "integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.

Mental Health

Information for the NICS

On January 4, 2016, the Department of Health and Human Services (HHS) modified the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a firearm.

The final rule gives states improved flexibility to ensure accurate but limited information is reported to the NICS. This rulemaking makes clear that, under the Privacy Rule, certain covered entities are permitted to disclose limited information to the NICS. The information that can be disclosed is the minimum necessary identifying information about individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs.

An individual who seeks help for mental health problems or receives mental health treatment is not automatically legally prohibited from having a firearm; nothing in this final rule changes that.

CONTINUED >>>

Protected Health Information (PHI)

What is Protected Health Information (PHI)?

Under the HIPAA Privacy Rule, protected health information, or "PHI," refers to individually identifiable health information that is created, received, stored, or transmitted in any form or medium by a covered entity or their business associate in relation to the provision of healthcare, healthcare operations and payment for healthcare services. Individually identifiable health information is that which can be linked to a particular person. Specifically, this information can relate to:

- The individual's past, present or future physical or mental health or condition;
- The provision of health care to the individual; or,
- The past, present, or future payment for the provision of health care to the individual; or
- The individual's genetic information.

PHI includes 18 identifiers that can be used to identify a patient, including:

- Name
- Address (including subdivisions smaller than state such as street address, city, county, or zip code)
- Any dates (except years) that are directly related to an individual, including birthday, date of admission or discharge, date of death, or the exact age of individuals older than 89
- Telephone and fax numbers
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers, serial numbers, or license plate numbers
- Device identifiers or serial numbers
- IP address and Web URLs
- Biometric identifiers such as fingerprints or voice prints
- Full-face photos
- Any other unique identifying numbers, characteristics, or codes

What is Electronic Protected Health Information (ePHI)?

"Electronic Protected Health Information" or "ePHI" means Protected Health Information that is maintained in or transmitted by electronic media.

Uses & Disclosures of PHI

Covered entities must safeguard PHI by implementing policies and procedures to restrict access to and use of PHI. Furthermore, a covered entity must only use or disclose the minimum amount of PHI necessary.

Required disclosures include:

- To an individual when requested & required by Section 164.524 (Access) & Section 164.528 (Accounting)
- To HHS, to investigate or determine compliance with Privacy Rule
- To the FBI and the National Instant Criminal Background Check System (NICS) for mental health issues regarding gun possession

Besides required disclosures, covered entities also may disclose PHI to their patients / health plan enrollees so that:

- Health plans can contact their enrollees, and
- Providers can talk to their patients

Permitted Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) provided to the individual (unless required for access or accounting of disclosures); (2) used for treatment, payment, and health care operations; (3) granting opportunity to agree or object; (4) as an incident to an otherwise permitted use and disclosure; (5) for public interest and benefit activities; and (6) as a limited data set for the purposes of research, public health or health care operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Breach Notification

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) requires HIPAA-covered entities and business associates to follow specific rules relating to the discovery of a breach of protected health information. These rules require covered entities and business associates to do the following when a security breach is discovered:

- Provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information.
- Provide notice to prominent local media outlets if there is a breach affecting more than 500 residents of a state or jurisdiction.
- In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach.

A "breach" is defined as the acquisition, access, use, or disclosure of protected health information in an impermissible manner which compromises its security or privacy.

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

The covered entity must send the required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered.

CONTINUED >>>

Anti-Discrimination Notice

General

Under current law, a group health plan may not establish any rule for eligibility (including continued eligibility) of any individual to enroll for benefits under the terms of the plan that discriminates based on any health factor that relates to that individual or a dependent of that individual.

Health Factors

The term "health factor" means, in relation to an individual, any of the following health status-related factors:

- Health status;
- Medical condition (including both physical and mental illnesses);
- Claims experience;
- Receipt of health care;
- Medical history;
- Genetic information;
- Evidence of insurability (including conditions arising out of acts of domestic violence or out of participations in recreational activities);
- Disability.

Eligibility Rules

Rules for eligibility include rules relating to any of the following:

- Enrollment;
- The effective date of coverage;
- Waiting (or affiliation) periods;
- Late and special enrollment;
- Eligibility for benefit packages;
- Benefits (including copayments and deductibles);
- Continued eligibility;
- Terminating coverage (including disenrollment) of any individual under the plan.

Nonconfinement and Actively-At-Work Provisions

A plan may not establish a rule for eligibility or set any individual's premium or contribution rate based on whether an individual is confined to a hospital or other health care institution or whether the individual is actively at work (including continuous employment).

Similarly Situated Individuals

Distinctions among groups of similarly situated individuals may not be based on a health factor. Group health plans may limit or exclude coverage or benefits if the restriction is applied uniformly to all similarly situated individuals and is not directed at any individual participants or beneficiaries based on a health factor.

Exceptions for Wellness Programs

Special rules and exceptions apply to wellness programs (programs designed to promote health or prevent disease) that provide benefit incentives.