What does HIPAA do?

HIPAA, or the Health Insurance Portability and Accountability Act, referred to as "the Rule" in this FAQ, creates national standards to protect individuals' medical records and other personal health information.

- 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.
- 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 limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It gives patients the right to examine and obtain a copy of their own health records and request corrections.

Can telemarketers obtain my health information and use it to call me to sell goods and services?

No, not without written authorization. Under HIPAA, a covered entity can share protected health information for marketing and sale only if it has obtained the individual's prior written authorization to do so.

Does HIPAA require my doctor to send my medical records to the government?

No. The Rule does not require a physician or any other entity to send medical information to the government for a government data base or similar operation. It does not require or allow any new government access to medical information, with one exception: the Rule does give the U.S. Department of Health and Human Services Office for Civil Rights (OCR) the authority to investigate complaints that Privacy Rule protections or rights have been violated, and otherwise to ensure that covered entities comply with the Rule.

Will this legislation or HIPAA make it easier for police and law enforcement agencies to get my medical information?

No. The Rule does not expand current law enforcement access to individually identifiable health information. The Rule establishes procedures and safeguards that restrict the circumstances under which a covered entity may give such information to law enforcement officers.

For example, the Rule limits the type of information that entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Similarly, under most circumstances, the Privacy Rule requires covered entities to obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement.

When does HIPAA allow providers or other entities covered by the law to disclose protected health information to law enforcement officials?

HIPAA is balanced to protect an individual's privacy while allowing important law enforcement functions to continue. The Rule permits entities to disclose protected health information (PHI) to law enforcement officials, without the individual's written authorization, under specific circumstances summarized below:

- **To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena.** The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information.
- **To respond to an administrative request***,* such as an administrative subpoena or investigative demand or other written request from a law enforcement official.
- **To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures** of PHI to name and 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, and a description of distinguishing physical characteristics. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request.

  This same limited information may be reported to law enforcement:

  - **About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity's workforce**
  - **To identify or apprehend an individual who has admitted participation in a violent crime** that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual's request for therapy, counseling, or treatment related to the propensity to commit this type of violent act.
- **To respond to a request for PHI about a victim of a crime, and the victim agrees**. If, because of an emergency or the person's incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree,

and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested.

Where child abuse victims or adult victims of abuse, neglect or domestic violence are concerned, other provisions of HIPAA apply:

  - **Child abuse or neglect may be reported** to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required.
  - **Adult abuse, neglect, or domestic violence may be reported** to a law enforcement official authorized by law to receive such reports,
    - If the individual agrees;
    - If the report is required by law; or
    - If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations.
    - Notice to the individual of the report may be required.
- **To report PHI to law enforcement when required by law** to do so. For example, state laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and both HIPAA and MHRA permits disclosures of PHI as necessary to comply with these laws.
- **To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.**
  - Information about a decedent may also be shared with medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties.
- **To report information that an entity governed by HIPAA believes to be evidence of a crime that occurred on its premises**.
- **When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity,** specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime. This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence.
- When consistent with applicable law and ethical standards:
  - To a law enforcement official reasonably able to **prevent or lessen a serious and imminent threat to the health or safety of an individual or the public**; or
  - **To identify or apprehend an individual who appears to have escaped from lawful custody**.
- **For certain other specialized governmental law enforcement purposes**, such as:
  - **To federal officials authorized to conduct** intelligence, counter-intelligence, and other national security activities under the National Security Act or to provide protective services to the President and others and conduct related investigations.
  - **To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody** of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the health and safety of the individual, other inmates, officers or employees of or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility.

Except when required by law, the disclosures to law enforcement summarized above are subject to a minimum necessary determination by the covered entity. Moreover, if the law enforcement official making the request for information is not known to the entity, the entity must verify the identity and authority of such person prior to disclosing the information.

Does the HIPAA Privacy Rule protect genetic information?

Yes, genetic information is health information protected by HIPAA.

Does the HIPAA Privacy Rule limit what a doctor can do with a family medical history?

Yes. When a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual's family medical history, this information becomes part of the individual's medical record and is treated as "protected health information" about the individual. Thus, the individual (and not the family members included in the medical history) may exercise the rights under the HIPAA Privacy Rule to this information in the same fashion as any other information in the medical record, including the right of access, amendment, and the ability to authorize disclosure to others.

Would this legislation change whether debt collectors or others can pursue patients for bills?

No. HIPAA already permits entities to share medical information for the purposes of facilitating payment for services, and entities are held to a "minimum necessary" standard with respect to releasing information. This legislation simply removes the requirement in state statute to seek a proactive consent from the patient, which 99% of patients today already agree to provide. In addition to the privacy protections for bill collection and payment activities under HIPAA, Minnesota's providers are also held to strict billing and collection standards under other laws, including the Fair Debt Collections Practices Act, and Affordable Care Act.

Would this legislation enable law enforcement entities to request and receive medical information for purposes like denying a permit for a firearm, or seizing a firearm from a patient?

No. As described above, under HIPAA, the permitted releases of information to law enforcement are specific, limited, and place conditions on what information can be shared. None of the law enforcement exceptions would permit law enforcement to obtain records without a warrant or court order for the administration of firearm permits. It is important to note that there are existing federal and state laws that govern when a provider has a duty to warn, requires a release of limited information to law enforcement, or authorizes an exception to consent if there is an imminent threat of risk or harm, but HF 3312/SF 2975 does not alter those requirements.