
HIPAA: Responding to Orders, Subpoenas, and Law Enforcement



Kim C. Stanger
(8-17)

Preliminaries

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

Overview

- **Does HIPAA even apply?**
- **Rules for disclosures**
 - Authorizations
 - Mandatory disclosures
 - Court orders, warrants and subpoenas
 - Disclosures to law enforcement
- **Law enforcement access to patients**
- **Suggestions for applying the rules.**

Written Materials

- **OCR, HIPAA Privacy Rule: Guide for Law Enforcement**
- **H&H Client Alert, *Valid Authorizations: A Checklist***
- **H&H Client Alert, *Responding to Subpoenas, Orders, and Administrative Demands***
- **H&H Client Alert, *Disclosures to Law Enforcement***
- **Sample Documents**
 - Letter to person who requested PHI without satisfying HIPAA
 - Letter to patient who is subject of subpoena

Preliminaries

- **This is an overview of relevant laws.**
- **There may be additional laws or ordinances.**
 - **Federal or state laws requiring or prohibiting disclosures.**
- **HIPAA preempts less restrictive state laws.**
- **Response is often fact-specific.**

Preliminaries

- Submit questions via chat feature or directly to kcstanger@hollandhart.com.
- The session will be recorded and available for download at <http://www.hhhealthlawblog.com/webinar-recordings-and-presentations>.

Health Insurance Portability and Accountability Act (“HIPAA”)



HIPAA:

General Rules

- **Covered entity or business associate may not use or disclose protected health information unless:**
 - **Written authorization from patient or personal representative;**
 - **Use or disclosure for treatment, payment or healthcare operations; or**
 - **Another HIPAA exception applies.**

(45 CFR 164.502).

Problem

- Person demanding info (attorney, prosecutor, officer) may not understand or care about HIPAA.
 - They are not subject to HIPAA.
 - Their job is to get the info they need, not help you comply with HIPAA.
 - They may tell you things that are not accurate.
- But you are still subject to HIPAA...



HIPAA Civil Penalties

| Conduct | Penalty |
|---|---|
| Did not know and should not have known of violation | <ul style="list-style-type: none">• \$100 to \$50,000 per violation• Up to \$1.5 million per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty |
| Violation due to reasonable cause | <ul style="list-style-type: none">• \$1000 to \$50,000 per violation• Up to \$1.5 million per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty |
| Willful neglect, but correct w/in 30 days | <ul style="list-style-type: none">• \$10,000 to \$50,000 per violation• Up to \$1.5 million per type per year• Penalty is mandatory |
| Willful neglect, but do not correct w/in 30 days | <ul style="list-style-type: none">• At least \$50,000 per violation• Up to \$1.5 million per type per year• Penalty is mandatory |

HIPAA Criminal Penalties

- Applies if employees or other individuals obtain or disclose protected health info from covered entity without authorization.

| Conduct | Penalty |
|--|---|
| Knowingly obtain info in violation of the law | <ul style="list-style-type: none">• \$50,000 fine• 1 year in prison |
| Committed under false pretenses | <ul style="list-style-type: none">• 100,000 fine• 5 years in prison |
| Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm | <ul style="list-style-type: none">• \$250,000 fine• 10 years in prison |

Additional Consequences

- **State attorney general may sue for HIPAA violations.**
 - \$25,000 per violation + costs
- **Individuals may assert common law tort claim.**
- **Must self-report breaches of unsecured protected health info.**
 - To the individual.
 - To HHS.
- **Must impose sanctions against members of workforce who violate HIPAA.**
- **Adverse licensure action.**

HIPAA Analysis



**Does HIPAA
apply?
If so, what must
I do?**



HIPAA Analysis

- **Does HIPAA apply to the request?**
 - Are you a covered entity or business associate?
 - Does the request seek protected health info?
- **Does HIPAA allow disclosure?**
 - Does the person have authority to request the info?
 - Is there a HIPAA authorization allowing disclosure?
 - Does a HIPAA exception allow the disclosure?
- **Even if HIPAA allows disclosure, should you make the disclosure?**
 - Does another law require or prohibit disclosure?
 - Have you limited the disclosure to the minimum necessary?

Does HIPAA Apply?

- **HIPAA applies to:**
 - **Covered entities**
 - Healthcare providers who engage in certain electronic transactions.
 - Health plans, including group health plans if:
 - 50 or more participants, or
 - Administered by a third party.
 - Healthcare clearinghouses.
 - **Business associates of covered entities**
 - Create, receive, maintain or transmit protected health info on behalf of the covered entity.
- **HIPAA does not apply if provider is not acting in its capacity as a healthcare provider, e.g., as employer.**

Does HIPAA Apply?

- **HIPAA applies to protected health info (“PHI”)**
 - Info that may reasonably be used to identify an individual.
 - Relating to health, health care or payment.
 - Medical records, bills, info obtained during treatment.
 - NOT info unrelated to health care or payment.
 - Created or maintained by covered entity.
 - Applies to records created by other providers.
 - In any form or medium.
 - Paper, electronic, oral, etc.
- **HIPAA does not apply to other info even though it may be confidential, e.g., employment records, incident reports not involving patients, etc.**

HIPAA: General Rules

- **Covered entity and business associates may not use or disclose PHI unless:**
 - **For purposes of treatment, payment or healthcare operations.**
 - **Have written, HIPAA-compliant authorization.**
 - **An exception applies that allows disclosures.**

(45 CFR 164.502)

HIPAA: General Rules

- **Potentially relevant exceptions**
 - Disclosures to avert serious harm.
 - Disclosures required by law.
 - Disclosures in administrative or judicial proceeding.
 - Court order or warrant signed by judge
 - Grand jury subpoena
 - Subpoena if certain conditions satisfied
 - Disclosures to law enforcement.
 - Facility directory
 - Report a crime
 - Locate victim, suspect, fugitive, etc.
 - Others

(45 CFR 164.510 and 164.512)

Written Authorization



Written Authorization

- **May disclose PHI with patient's or personal rep's written authorization.**
 - Must contain required elements.
 - Must contain required statements.
- **Authorization may not be combined with other documents.**

(45 CFR 164.508)

Written Authorization

- **Required Elements**
 - Written in plain language.
 - Describe PHI to be disclosed.
 - Identify entity authorized to make disclosure.
 - Identify entity to whom disclosure made.
 - Describe purpose of disclosure.
 - “At request of individual” if patient initiates.
 - Include expiration date or event.
 - Dated and signed by patient or representative.
 - State authority of personal representative.

Written Authorization

- **Required Statements**
 - Right to revoke the authorization in writing at anytime and either:
 - Describe exceptions and how to revoke, or
 - Refer to Notice of Privacy Practices where such info may be found.
 - Cannot condition treatment or payment on authorization.
 - PHI may be re-disclosed and, if so, may not be protected.

(45 CFR 164.508)



NEW

Written Request to Send Info to Third Party

- Patient has right to direct that PHI be sent to third party.
- Request must:
 - Be in writing (e.g., paper, electronic, portal)
 - Signed by patient or personal rep
 - Clearly identify the recipient
 - Clearly identify where records to be sent.
- Limits applicable to patient apply to such requests.
 - Must respond within 30 days.
 - Must provide in form and format requested.
 - May only charge a reasonable cost-based fee.
- Must take reasonable steps to protect the PHI in transit.

(45 CFR 164.524)



Practical Application: Document Patient's Consent

- As a practical matter, if you get the patient's or personal rep's request or consent to make the disclosure and document it, you're likely going to be safe.
 - May be technical violation of written requirements.
 - No “willful neglect”= no penalties.
- Make sure you document it.
 - Letter or communication from or to patient.
 - Medical record.
- *Beware situations in which court or police don't want patient alerted.*

Disclosures to Avert Serious Harm



Disclosures To Avert Serious Harm

- **May disclose info if provider believes in good faith that the disclosure is:**
 - Necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
 - Made to a person reasonably able to prevent or lessen the threat, including the target of the threat; and
 - Consistent with applicable law and ethical conduct.
- **Provider presumed to act in good faith if based on:**
 - provider's actual knowledge, or
 - credible representation by someone with apparent knowledge or authority.

(45 CFR 164.512(j)(1)(i), (3))

Disclosures Required by Law



Disclosures Required by Law

- **May disclose PHI to the extent another law requires disclosure.**
 - Disclose to appropriate entity.
 - Limit disclosure to scope of the law.

(45 CFR 164.512(a) and 164.512(f)(1)(i))

- **This does not apply if the other law simply permits disclosure.**
 - E.g., statute allows disclosure of info to Dept. of Transportation re condition that affects driving.

(78 FR 5618)

Common Laws Requiring Disclosure

- **Births and deaths**
 - See also 45 CFR 164.512(b).
- **Certain communicable diseases**
 - See also 45 CFR 164.512(b).
- **Treatment of the victim of a crime**
- **Treatment of injury from a firearm**
 - See also 45 CFR 164.512(f)(1).
- **Mental health provider knows of threat to others**
- **Child abuse or neglect**
 - See 45 CFR 164.512(b)(ii).
- **Adult abuse or neglect**
 - See 45 CFR 164.512(c).

Disclosures Required by Law

Adult abuse, neglect or domestic violence

- Under HIPAA, may disclose info about abuse victim to govt agency:
 - If individual agrees to disclosure;
 - If and to extent disclosure is required by law; or
 - If and to extent disclosure is authorized by law, and (i) provider believes disclosure is necessary to avoid serious harm to victim; or (ii) if individual is incapacitated, law enforcement represents that info is not to be used against victim and immediate enforcement activity would be materially impaired by waiting.
- Must promptly inform patient or personal rep of disclosure unless:
 - Provider believes that informing patient would place the individual at risk of serious harm; or
 - If disclosure would be to the personal rep, provider believes the personal rep is responsible for the abuse, neglect or other injury, and that it is not in best interest of patient to disclose the info.

(45 CFR 164.512(c))

Disclosures Required by Law

Theft of Controlled Substance

- Registrants must notify the DEA Field Division Office in their area, in writing, of the theft or significant loss of any controlled substance within one business day of discovery of such loss or theft.
- Complete and submit to the Field Division Office in their area, DEA Form 106, "Report of Theft or Loss of Controlled Substances" regarding the theft or loss.
- Failure to report may result in adverse action against DEA registration.

(DEA Diversion Control Program; 21 CFR 1301.76(b))



U.S. DEPARTMENT OF JUSTICE ★ DRUG ENFORCEMENT ADMINISTRATION OFFICE OF DIVERSION CONTROL

Search



REPORTING > Reports Required by 21 CFR > Theft or Loss of Controlled Substances - DEA Form 106

Theft or Loss of Controlled Substances - DEA Form 106

IMPORTANT NOTICE: Only those persons registered with DEA to handle controlled substances may utilize this form.

Federal regulations require that registrants notify the DEA Field Division Office in their area, in writing, of the theft or significant loss of any controlled substance within one business day of discovery of such loss or theft. The registrant shall also complete and submit to the Field Division Office in their area, DEA Form 106, "Report of Theft or Loss of Controlled Substances" regarding the theft or loss. (**21 C.F.R. § 1301.76(b)**)

DEA controlled substance registrants are strongly encouraged to complete and submit the DEA Form 106 online. In addition to being more convenient, completing the form online results in fewer errors. A link to the online DEA Form 106 is provided below.

In order to better track controlled substances reported as lost or stolen, DEA has incorporated use of the National Drug Code (NDC) number in the DEA Form-106. The NDC number identifies the manufacturer, product, dosage form, and package size. Entry of the NDC number will prompt the system to auto-populate additional fields such as the name of the product, dosage form, dosage strength, and quantity per container.

If a registrant does not have internet access, a paper copy of the DEA-106 form can be requested by writing to:

Drug Enforcement Administration
Attn: Regulatory Section/ODG
8701 Morrisette Drive
Springfield, VA 22152

For more information regarding reporting theft or loss of controlled substances, see the Federal Register Notice - "[Reports by Registrants of Theft or Significant Loss of Controlled Substances.](#)"

DEA Form106

Data will be entered through a **secure connection** to the online application system. **Your web browser must support 128-bit encryption.**

If you have questions regarding the electronic submission of the DEA Form-106, please contact **DEA Call Center 1-800-882-9539.**

Privacy Act Information for DEA Form 106

- Authority:** Section 301 of the Controlled Substances Act of 1970 (PL-513).
Purpose: Report theft or loss of Controlled Substances.
Routine Uses: The Controlled Substances Act authorizes the production of special reports required for statistical and analytical purposes. Disclosures of information from this system are made to the following categories of users for the purposes stated:
1. Other Federal law enforcement and regulatory agencies for law enforcement and regulatory purposes.
 2. State and local law enforcement and regulatory agencies for law enforcement and regulatory purposes.
- Effect:** Failure to report theft or loss of controlled substances may result in penalties under Section 402 and 403 of the Controlled

- ARCOS
- BCM Online
- Chemical Import/Export Declarations
- CSOS (Controlled Substances Ordering System)
- Drug Theft/Loss Import/Export
- Inventory of Drugs Surrendered
- Quotas
- Reports Required by 21 CFR
- Submit a Tip to DEA
- Year-End Reports

Disclosures that May or May Not Be Required by Law

- Dog bites
 - Traffic accidents
 - Criminal behavior
 - Pregnant mother's use of drugs
 - Sex involving minor
 - Others?
-
- *Check state laws and local ordinances.*
 - *When in doubt, ask for citation to authority requiring disclosures.*

Orders, Warrants or Administrative Requests



Orders, Warrants or Administrative Requests

- **Judicial proceeding**
 - Civil or criminal
 - Federal or state court (e.g., U.S. District Court, state court, etc.)
 - Usually signed by judge or magistrate
- **Administrative proceeding**
 - Action involving administrative agency (e.g., HHS, CMS, OIG, state department of health, etc.)
 - Usually signed by administrative law judge, hearing officer, etc.

Order or Warrant

- **May disclose PHI in response to an order or warrant signed by:**
 - **A judge or magistrate.**
 - **An administrative law judge or administrative tribunal.**
- **Limit the disclosure to the PHI expressly authorized by the order or warrant.**

(45 CFR 164.512(e)(1)(ii))

- **The judge = the law.**

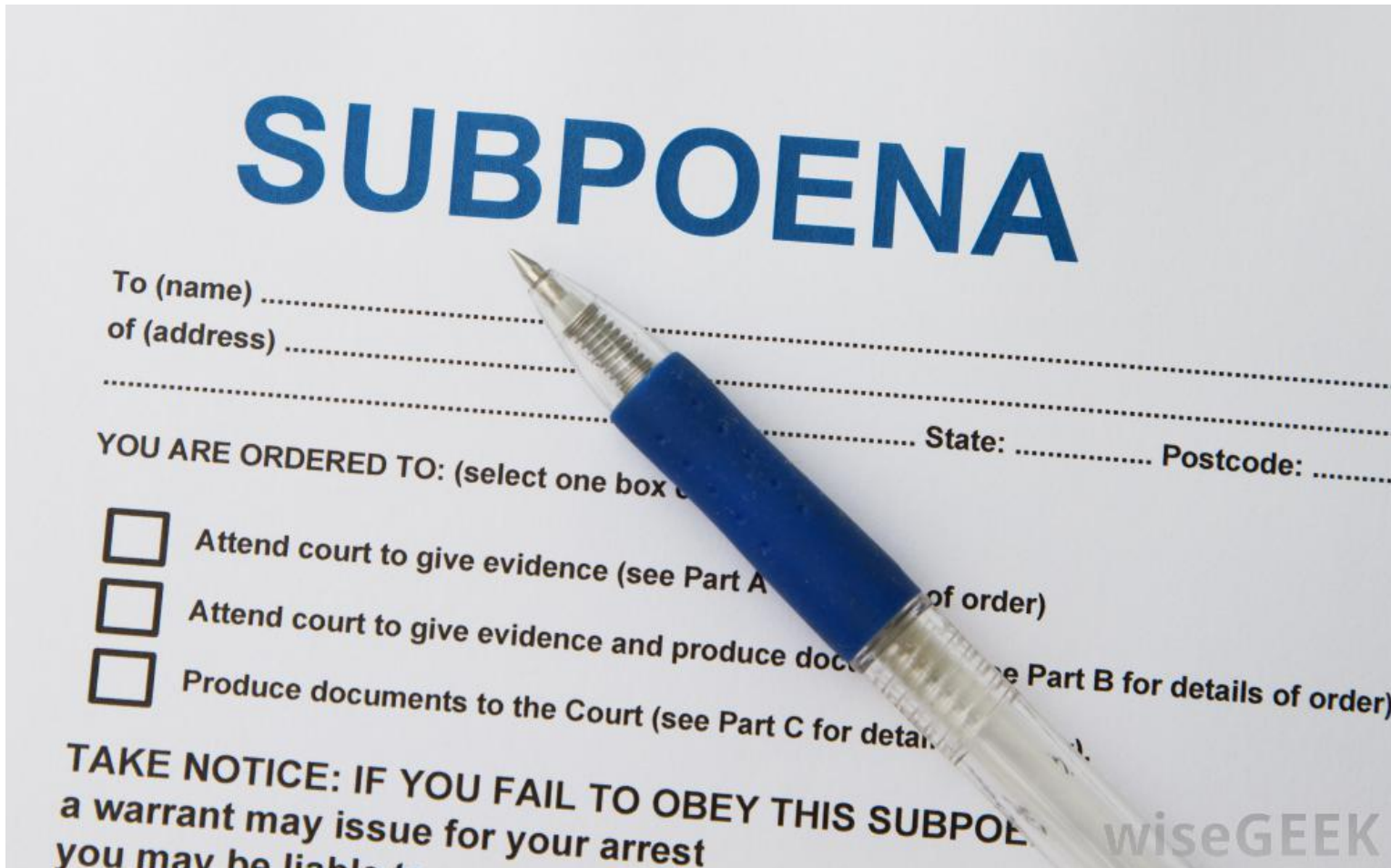
Administrative Requests

- **May disclose per administrative request, subpoena, summons or demand authorized by law if:**
 - **Info relevant and material to legitimate law enforcement inquiry;**
 - **Request is reasonably specific and limited to purpose; and**
 - **De-identified info could not be used.**
- (45 CFR 164.512(f)(1)(ii))
- **Additional protections required because no independent judicial officer is involved.**

Order or Warrant

- **Must petition court if decline to provide info; otherwise, may be subject to contempt sanctions.**
- **May consider whether the court has jurisdiction.**
 - **State court: generally limited to state.**
 - **Federal court: depends.**
- **If in doubt, check with the court or your attorney.**

Subpoenas



Subpoenas

- Subpoenas are issued by courts or administrative tribunals to compel attendance or production.
 - Subpoena: attend trial, deposition or other proceeding
 - Subpoena *duces tecum*: bring or produce documents
- May be issued by:
 - Judge or magistrate
 - Prosecutor
 - Lawyer
 - Administrative officer
 - Other

**Rules differ
depending on who
signs subpoena**

Subpoena: Signed by Judge or Magistrate

- **May disclose PHI per subpoena signed by judicial officer judge or magistrate.**

(45 CFR 164.512(e)(1)(i))

- **“Judicial officer” not defined, but means**
 - **Judge, magistrate, or administrative judge**
 - **Impartial, independent officer**
 - **NOT prosecutor, attorney, or court clerk.**
 - **Not impartial or independent**
- **The judge = the law.**

Grand Jury Subpoena

- **May disclose PHI per grand jury subpoena.**
(45 CFR 164.512(e)(1)(i))
- **Everything that takes place before a grand jury is confidential.**

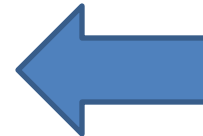
AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury

UNITED STATES DISTRICT COURT

for the

District of New Jersey

SUBPOENA TO TESTIFY BEFORE A GRAND JURY



To:

YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.



Subpoena: NOT Signed by Judge or Magistrate

- Do not ignore subpoena if court has jurisdiction.
- Cannot disclose PHI unless satisfy one of following:
 - Receive written satisfactory assurances that patient notified of subpoena, given chance to object, and either objections have been denied or time has elapsed;
 - Subpoena itself may contain such assurances.
 - Qualified protective order requested or in place; or
 - Make reasonable efforts to contact patient yourself.
 - See sample letter.



(45 CFR 164.512(e)(1)(ii))

Responding to Order or Subpoena

- Does it require disclosure of PHI?
- Does the court that issued it have jurisdiction?
 - State court: from state in which you are located.
 - Fed court: check with attorney.
- Who signed it?
 - If judge or magistrate: comply with order or subpoena.
 - If NOT judge or magistrate:
 - Notify patient that you must respond unless patient quashes subpoena.
 - If insufficient time, contact party issuing subpoena to explain HIPAA limits, get more time, etc., but be careful not to disclose PHI.
 - File motion to quash, but this too expensive.
 - Appear and assert HIPAA objection.
- What does it require?

Responding to Subpoena

- **Comply with strict terms of subpoena or order.**
 - Don't disclose more PHI than is specified.
 - Disclose only in manner specified.
 - If subpoena requires records, produce records.
 - If subpoena requires attendance, respond appropriately.
 - Don't disclose PHI in discussions outside scope of subpoena.
- **If pressed, explain HIPAA limits.**
- **When in doubt, check with your own attorney.**
- **Log response in accounting of disclosure log required by 45 CFR 164.528.**

Law Enforcement



HIPAA and Law Enforcement

- Law enforcement = federal law enforcement, police, prosecutors, Dept. of Justice, etc.
- HIPAA applies to law enforcement requests, i.e., to disclose, must have—
 - Patient’s authorization,
 - Treatment purposes, or
 - A valid HIPAA exception.

(See 45 CFR 164.502; 164.512(f))

Disclosures to Apprehend Person

- May disclose PHI if provider believes in good faith that the disclosure is necessary for law enforcement to identify or apprehend an individual:
 - Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim, or
 - It appears that individual has escaped from a correctional institution or from lawful custody.
- Does not apply if info learned through treatment of propensity to commit the act.

(45 CFR 164.512(j)(1)(ii))

Facility Directory

- **May disclose limited info as part of a facility directory if:**
 - **Informed the patient that provider would include info in facility directory and gave the patient the chance to restrict disclosures (e.g., in notice of privacy practices) and patient did not object.**
 - **Requestor asks for the person by name.**
- **Disclosure limited to:**
 - **Patient's name.**
 - **Patient's location in facility.**
 - **Patient's general condition.**

(45 CFR 164.510)

Health Oversight

- **May disclose to health oversight agency for oversight activities authorized by law.**
 - **Includes audits; investigations; inspections; or civil, criminal, or administrative proceedings.**
 - **Relates to**
 - **Oversight of health care system.**
 - **Eligibility for benefits under government programs.**
 - **Compliance with government programs.**
 - **Compliance with civil rights laws.**
 - **Does not apply to investigations of individual unrelated to provision of health care or claim for health care benefits.**

(45 CFR 164.512(d))

Law Enforcement Orders

- **May disclose per**
 - **Court order, warrant, subpoena or summons issued by a judicial officer.**
 - **i.e., signed by judge or magistrate.**
 - **Grand jury subpoena.**
 - **Administrative request, subpoena, summons, demand or other process authorized by law if:**
 - **Info relevant and material to legitimate law enforcement inquiry;**
 - **Request is reasonably specific and limited to purpose; and**
 - **De-identified info could not be used.**

(45 CFR 164.512(f)(1)(ii))

Request to Identify or Locate Person

- Upon request from law enforcement, may disclose limited info to help identify or locate a suspect, fugitive, witness, or missing person.
 - Name and address
 - Date and place of birth
 - SSN
 - Blood type and rh factor
 - Type of injury
 - Date and time of treatment and death
 - Description of distinguishing characteristics (height, weight, race, hair color, facial hair, scars, tattoo, etc.)
 - Not info re DNA, dental records, or sample or analysis of body fluids or tissues.
- (45 CFR 164.512(f)(2))
- Applies to media alerts or “wanted” posters. (65 FR 85232)
 - Probably does not apply to general requests to notify them if they treat (e.g., MVAs) or when patient is released.

Victims of Crime

- Upon request from law enforcement, may disclose limited info about patient suspected to be victim of crime (other than abuse) if:
 - Patient agrees to disclosure, or
 - Unable to obtain patient's agreement because of incapacity or emergency and:
 - Law officer represents that info needed to determine violation of law by someone other than the patient and will not be used against the patient;
 - Law officer represents info needed immediately for law enforcement activity; and
 - Provider determines disclosure in best interests of individual.

(45 CFR 164.512(f)(3))

Decedents

- **If provider thinks that death resulted from a crime, provider may disclose info about decedent to law enforcement for the purpose of alerting law enforcement of the death.**

(45 CFR 164.512(f)(4))

Crime on Premises

- If provider thinks that crime has occurred on the premises, provider may disclose info that provider believes in good faith constitutes evidence of crime.

(45 CFR 164.512(f)(5))

Crime Off Premises

- If providing emergency care away from hospital, may disclose info if necessary to alert law enforcement to:
 - Commission and nature of crime (other than abuse);
 - Location of crime or of victims; and/or
 - Identity, description, and location of perpetrator.

(45 CFR 164.512(f)(6))

- Only applies to the extent you are rendering care, i.e., acting as healthcare provider.

Crime Against Workforce Member

- Provider not deemed to have violated HIPAA if a member of its workforce who is a victim of a crime discloses info to law enforcement if:
 - Info disclosed is about suspected perpetrator of crime, and
 - Info disclosed is limited to:
 - Name and address
 - Birthdate
 - SSN
 - Blood type
 - Type of injury
 - Date and time of treatment
 - Distinguishing physical characteristics

(45 CFR 164.502(j)(2))

Persons in Custody

- May disclose info about inmate or other person in custody to law enforcement or correctional facility if official represents that info necessary for:
 - Provision of health care to person;
 - Health and safety of individual or other inmates;
 - Health and safety of officers or employees at correctional facility;
 - Health and safety of officers transporting prisoner; or
 - Safety, security, and good order of correctional institution.
- Does not apply after the person is no longer a prisoner.

(45 CFR 164.512(k)(5))

Whistleblower

- **Provider is not deemed to have violated HIPAA if its workforce member discloses info if:**
 - **Workforce member believes in good faith that provider has violated the law or has endangered others, and**
 - **Disclosure is to a health oversight agency or authority authorized by law to investigate and respond.**

(45 CFR 164.502(j)(1))

Public Health Activities

- **May disclose for certain public health activities.**
 - **To public health authority authorized to receive info to prevent disease or injury.**
 - **To a person at risk of contracting or spreading disease if covered entity is authorized by law to contact person.**
 - **For certain FDA-related actions.**

(45 CFR 164.512(b))

Law Enforcement Access to Patients



TOPICS »

- Health Reform
- EHRs
- Medicare
- Liability
- AMA House
- » More

COLUMNS »

- Contract Language
- Ethics Forum
- In the Courts
- Practice Management
- Technically Speaking
- » More

LISTINGS

- Issue dates
- Regions
- Columns
- Archives
- Writers

HELP

- RSS
- Mobile
- Search tips
- Subscribe
- Staff directory
- Advertising
- Reprints
- Site guide
- Useful links
- About
- Contact

PARTNER LINKS

- AMA Wire
- CPT

GOVERNMENT

HIPAA allows police access to patients, federal judge rules

■ The case highlights the interplay between state and federal laws on sharing medical information about alleged crime victims, experts say.

By AMY LYNN SORREL — Posted May 21, 2007

PRINT | EMAIL | RESPOND | REPRINTS | LIKE | SHARE | TWEET

HIPAA privacy rules do not bar law enforcement from having access to patients who are victims of alleged crimes, a Louisiana federal judge recently ruled. The decision affirmed that police had the right to arrest a hospital case worker for obstruction of justice when she tried to stop police from questioning a patient.

The ruling likely will not embolden state authorities to barge into the treatment room, experts say.

"But the facts are perhaps a wake-up call," said Philip H. Lebowitz, a HIPAA lawyer and partner with Philadelphia-based Duane Morris LLP. "It does point out that what you might think is the right thing to do might not be under HIPAA."

Elizabeth Maier, the hospital employee at the center of the case, sued the police for falsely arresting her when she kept local police from seeing a patient who was being treated for alleged domestic abuse at Lafayette General Medical Center. The patient did not want to report the incident, but a nurse already had called 911, according to court records. Maier was never prosecuted.

During the encounter, Maier told police that HIPAA requires a patient's consent before disclosing private medical information. She argued in her lawsuit that the nurse who called the police to report the abuse had violated the patient's confidentiality under HIPAA. Maier also said police should have known she was just doing her job to protect the patient's privacy.

The police, on the other hand, argued that Louisiana law requires them to investigate reports of domestic violence once they are made and that Maier's actions prevented them from doing their duty.

Federal Judge Tucker L. Melancon agreed and dismissed Maier's lawsuit. He found that the officers had adequate reason to arrest Maier.

The privacy statute does not "prohibit hospital personnel from allowing

WITH THIS STORY:

- » Case at a glance
- » Related content

ADVERTISEMENT

Looking to drive state-level legislation?

The AMA Advocacy Resource Center can help.



ADVERTISE HERE

FEATURED

Confronting bias against obese patients

■ Medical educators are starting to raise awareness about how weight-related stigma can impair patient-physician communication and the treatment of obesity. [Read story](#)



Goodbye

■ *American Medical News* is ceasing publication after 55 years of serving physicians by keeping them informed of their rapidly changing profession. [Read story](#)



Policing medical practice employees after work

■ Doctors can try to regulate staff actions outside the office, but they must watch what they try to stamp out and how they do it. [Read story](#)



Diabetes prevention:



Police Access to Patients

- Private entities may generally require a warrant.
 - Cooperate with terms of warrant.
- Police may be able to access public areas without a warrant.
 - Consult with your attorney if this is problematic.
- Explain to police that, like other members of public, police are not given unrestricted access to patient care areas.
- Police are usually willing to cooperate.

Police Access to Patients

- *Work together to come up with workable solution!*



Police Access to Patients

- **If police want access to patient or facility:**
 - **Determine if access is appropriate considering:**
 - **Patient care concerns.**
 - **Provider operations.**
 - **Patient wishes.**
 - **Ask the patient if they consent to police access.**
 - **If patient agrees, provide access as appropriate.**
 - **If patient declines, explain to police.**
 - **Explain objections to police and work on solution.**

Police Access to Patients

- **If police insist on access despite objections.**
 - **Do not obstruct police action.**
 - **Do not lie or misrepresent facts to police.**
 - **Document objection, including parties involved and circumstances.**
 - **Complain to police officer's supervisor.**
 - **Work with police to develop protocol to avoid future problems.**

Applying the Rules



Applying the Rules: Orders, Warrants and Subpoenas

- **Signed by judge or magistrate:**
 - Comply or petition the court.
 - Limit disclosure to extent required.
- **Not signed by judge or magistrate:**
 - Notify patient and tell them you must respond unless they quash the order, warrant or subpoena.
 - Limit disclosure to extent required.
 - When in doubt, check with your attorney.

Applying the Rules: Law Enforcement

- If have concerns or questions about disclosure to law enforcement:
 - Explain same to law enforcement;
 - Voice and document objections; and/or
 - Ask for authority from law enforcement.
- **NEVER physically obstruct, misrepresent facts, or affirmatively hinder law enforcement efforts.**
 - May be liable for obstruction of justice.
- When in doubt, contact your attorney.

Prepare in Advance

- Include disclosures to per order, subpoena and law enforcement in Notice of Privacy Practices.
- Establish policy or process for responding.
 - Identify person responsible for contacting or responding to orders, subpoenas and law enforcement, e.g., privacy officer, charge nurse, administrator on call, or privacy officer.
 - Ensure privacy officer understands applicable rules.
 - Instruct personnel to notify responsible person ASAP.
- Work out process with law enforcement in advance.
- Train personnel concerning the process.
 - Limits on disclosures.
 - Process for disclosures.

Verify Authority of Requestor

- **Before disclosing protected info, covered entity must:**
 - Verify identity and authority of person requesting info if he/she is not known.
 - E.g., check the badge or papers of officers.
 - Obtain any documents, representations, or statements required to make disclosure.
 - E.g., representations from police that they need info for immediate identification purposes, or written satisfactory assurances accompanying a subpoena.
- **Does not apply to disclosures for purposes of facility directory where patient has not objected to disclosures.**
- **May rely on representations of officer if reliance is reasonable.**

(45 CFR 164.514(h))

Verify Authority of Requestor

- To be valid, court or administrative tribunal must have jurisdiction over entity to whom order, warrant, or subpoena is issued.
 - Federal court with jurisdiction in the state.
 - State court.
 - Generally not court from another state.
- May rely on representation of officer if reliance is reasonable.
- When in doubt, check with your attorney.

May Require Warrant

- In most cases, you are not required to respond to a law enforcement request absent a warrant, subpoena or court order.
 - The United States Constitution generally prohibits warrantless searches or seizures.
 - HIPAA exceptions generally allow, but do not require, disclosure.
- But be careful.
 - Usually want to cooperate with law enforcement.
 - State laws may require certain disclosures.
 - Do not physically interfere, lie to, or affirmatively hinder law enforcement if they proceed over your objection.

Informal Requests for Info

- **Generally need not respond to informal law enforcement request for info.**
- **Ask for basis or authority for request.**
- **Must have HIPAA exception to disclose info, e.g.,**
 - **Is disclosure to avert harm?**
 - **Is there a law that requires report to law enforcement?**
 - **Do we fit within one of the exceptions for disclosure to law enforcement?**

Object to Improper Disclosures

- Explain HIPAA requirements.
- Ask to speak with officer's supervisor.
- Contact your own attorney.
- Document your objections and police actions.
 - Names and badge numbers.
- Never physically interfere with law enforcement if they insist on acting despite your objection.

Minimum Necessary Standard

- **Even if HIPAA exception allows disclosure, you generally may not disclose more than is minimally necessary to accomplish intent.**

(45 CFR 164.504)

- **Limit disclosures to:**
 - **Extent disclosure required by law.**
 - **Scope of warrant, order or subpoena.**
 - **As necessary to accomplish purpose of disclosure.**

Log the Disclosure

- Providers must log most disclosures to law enforcement so that they may respond to patient's request for accounting of disclosures.
- Log must record:
 - Date of disclosure.
 - Name and address of entity receiving info.
 - Description of info disclosed.
 - Either a statement of purpose of disclosure or copy of the written request for disclosure (e.g., the order, subpoena, etc.).

(45 CFR 164.528)

Accounting of Disclosure

- Law enforcement or health oversight agency may suspend person's right to obtain accounting.
 - If written directive, the statement should:
 - Confirm accounting would be reasonably likely to impede agency's activities, and
 - State time for suspension.
 - If oral direction:
 - Provider must document direction, identity of agency or official.
 - Suspension limited to 30 days unless written statement obtained.

(45 CFR 164.528)

Report Breach of Unsecured PHI

- **Must report “breach” of unsecured PHI in violation of the HIPAA privacy rule to:**
 - Patient or personal representative.
 - Report within 60 days.
 - HHS.
 - If breach < 500 persons, may report within 60 days after calendar year.
 - If breach > 500 persons, must report at same time you notify individuals.
 - Local media, if breach > 500 persons in the state.

(45 CFR 164.400)

Report Breach of Unsecured PHI

- **Unauthorized access, use or disclosure of unsecured PHI is presumed to be a reportable breach unless provider can demonstrate that there is a low probability that the data has been compromised based on risk assessment of:**
 - **Type of info disclosed;**
 - **Entity to whom info disclosed;**
 - **Whether entity actually looked at the info; and**
 - **Actions taken to mitigate disclosure.**

(45 CFR 164.402)

Report Breach of Unsecured PHI

- May delay breach report to individual and HHS if law enforcement states that breach notification would impede criminal investigation or damage national security.
 - If statement in writing, may delay report for time period stated in writing.
 - If statement is oral, may delay for up to 30 days.
 - Document the statement, including identity of officer.
 - May request that written statement obtained in meantime.

(45 CFR 164.412)

Ensure Business Associates Comply

- **Business associate contract requires associates to comply with basic HIPAA requirements.**
- **Require business associates to immediately give provider notice of legal process or police requests.**
- **Not liable for business associate's violation unless:**
 - **Knew of violation and failed to act, or**
 - **Business associate is your agent.**

Consider Other Privacy Laws

- **Attorney client privilege.**
- **Work-product doctrine.**
- **Peer review privilege.**
- **Drug and alcohol treatment records.**
- **Others?**

Additional Resources



Resources

- **OCR, *HIPAA Privacy Rule: Guide for Law Enforcement***
- **H&H Client Alert, *Disclosures to Law Enforcement***
- **H&H Client Alert, *Responding to Subpoenas, Orders, and Administrative Demands***
- **AMA *Guidelines for Releasing Patient Info to Law Enforcement*, available on the internet**

www.hhs.gov/ocr/privacy/



HHS.gov

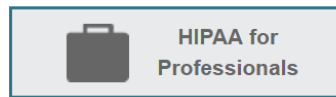
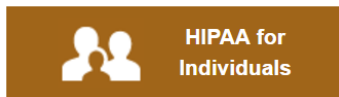
Health Information Privacy

U.S. Department of Health & Human Services

I'm looking for...



[HHS A-Z Index](#)



[HHS](#) > [HIPAA Home](#) > HIPAA for Professionals

- HIPAA for Professionals
- Privacy +
- Security +
- Breach Notification +
- Compliance & Enforcement +
- Special Topics +

Text Resize [A](#) [A](#) [A](#)

Print

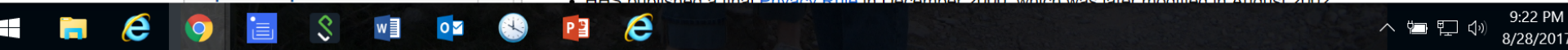
Share



HIPAA for Professionals

To improve the efficiency and effectiveness of the health care system, the [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

HHS published a final [Privacy Rule](#) in December 2000, which was later modified in August 2002.



<https://www.hollandhart.com/healthcare#overview>

Healthcare | Holland & H x

Secure | <https://www.hollandhart.com/healthcare#overview>

EXCELLENCE IN LEGAL SERVICES


MENU HOLLAND & HART 70 YEARS EST. 1947


OVERVIEW ▶

PRACTICES/INDUSTRIES

NEWS & INSIGHTS

CONTACTS


Kim Stanger
Partner
Boise


Blaine Benard
Partner
Salt Lake City

HEALTH LAW BLOG
Access to previous webinar recordings, publications, and more.

The Healthcare Industry is positioning this sector now making up clients stand ready to help as changes

Issues such as rising healthcare costs, innovations in healthcare delivery, demands on the minds of many of our clients. We are seizing opportunities that arise in this dynamic environment.

Clients We Serve

- Hospitals
- Individual medical providers
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs)
- Health information exchanges (HIEs)
- Practice managers and administrators

Past Webinars

Publications

- Ambulatory surgery centers
- Medical device and life science companies



Questions



Kim C. Stanger

kcstanger@hollandhart.com

(208) 383-3913