Legal Aspects of Forensic Photography

Nolan S. Young,
Arent Fox LLP
Patient/Victim Privacy

Los Angeles Times | ARTICLE COLLECTIONS

YOU ARE HERE: LAT Home → Collections → Assaults

Rihanna photo prompts LAPD probe

The department is investigating whether the image of the battered singer was leaked to TMZ from within. She was allegedly assaulted by her pop star boyfriend Chris Brown.

February 21, 2009 | Joel Rubin and Richard Winton

Los Angeles Police Department officials on Friday were interviewing officers and scouring electronic records amid growing suspicion that someone inside the department leaked or sold to a celebrity website a photo of the singer Rihanna that depicted injuries to her face she suffered during an alleged assault by her boyfriend.

Police officials said it appears the photo is part of the LAPD’s ongoing investigation of Chris Brown, the pop star who allegedly assaulted the singer in the early morning the day of the Grammy Awards two weeks ago.
Patient/Victim Privacy

• It was humiliating; that is not a photo you would show to anybody. I felt completely taken advantage of. I felt like people were making it into a fun topic on the Internet, and it’s my life. I was disappointed, especially when I found out the photo was [supposedly leaked by] two women.
Overview

• Patient’s Right to Privacy
  – Health Insurance Portability and Accountability Act ("HIPAA")
  – The Health Information Technology for Economic and Clinical Health ("HITECH") Act
  – State Laws

• Informed Consent
  – What is Required?
  – Consent for treatment vs. consent for disclosure.

• Trends
  – Increased Enforcement
  – Encryption
  – Whose Record is it?
Patient’s Right to Privacy
Patient/Victim Privacy

• Two primary sources of privacy laws that you need to consider when developing institutional policies:
  – Federal HIPAA Regulations
  – State Laws
    • State Health Information Technology Laws
    • State Reporting Requirements
HIPAA
HIPAA

• HIPAA
  – General Provisions
  – Privacy Rule - “Establishes . . . a set of [minimum] national standards for the protection of certain health information.”
  – Security Rule - “Establishes a national set of [minimum] security standards for protecting certain health information that is held or transferred in electronic form.”
  – Breach Notification Requirements (HITECH Act)
HIPAA General Provisions

• To Whom does HIPAA Apply?
  – “Covered Entities”
    • Virtually all health care providers – all health care providers who transmit health information electronically in connection certain transactions including the transmission of claims, benefit eligibility inquiries, referral authorization requests, etc.
    • The use of electronic technology such as email is not enough
Are You a Covered Health Care Provider?²

Do you furnish, bill or receive payment for, health care in the normal course of business?

No

STOP
You are NOT a covered health care provider

Yes

Do you transmit information electronically in connection with specified transactions including claims, eligibility, referral authorizations, etc.

Yes

You ARE a covered entity
HIPAA Privacy Rule

- **Objective** - assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.

- The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.
HIPAA Privacy Rule

• The Basic Principle of the Privacy Rule - A covered entity may not use or disclose protected health information, except:
  – as specifically permitted or required by the Privacy Rule; or
  – as authorized *in writing*, by the individual who is the subject of the information.
HIPAA Privacy Rule

• What information is protected
  – all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
Protected Health Information

• “Individually identifiable health information” is information, including demographic data, that relates to:
  – the individual’s physical or mental health or condition,
  – the provision of health care to the individual, or
  – the payment for the provision of health care to the individual

- AND -

- that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g. name, address, birth date, Social Security Number).
Permitted Uses and Disclosures

1. Uses and disclosures for which authorization is not required *(some require consent)*:
2. Uses and disclosures for which the opportunity to agree or object is required;
3. Uses and disclosures for which authorization is required.
Permitted Uses and Disclosures

1. Uses and disclosures for which authorization is not required (some require consent):
   – Disclosures to carry out treatment, payment, or healthcare operations;
   – Disclosures required by law;
   – Disclosures for public health activities;
   – Disclosures about victims of abuse, neglect or domestic violence;
   – Disclosures for health oversight activities;
   – Disclosures for judicial and administrative proceedings;
   – Disclosures for law enforcement purposes;
Required Disclosures

• HIPAA Requires Disclosures only in the following situations:
  – Disclosure to the individual that is the subject of protected health information when that individual specifically requests the information;
  – Disclosure to the United States Department of Health and Human Services (“HHS”) is required when it is undertaking a compliance investigation or review or enforcement action.

• Note - Disclosure could be required by state law under other circumstances
Permitted Uses and Disclosures

1. Uses and disclosures for which authorization is not required (continued):
   - Disclosures about decedents;
   - Disclosures for cadaveric organ, eye or tissue donation purposes;
   - Disclosures for research purposes;
   - Disclosures to avert a serious threat to health or safety;
   - Disclosures for specialized government functions;
   - Disclosures for workers compensation.
Permitted Uses and Disclosures

Disclosures required by law

- Many states have laws that require medical personnel to report information related to certain injuries or offenses, including protected health information, to relevant authorities.

- Under HIPAA, a covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure is limited to the relevant requirements.
Permitted Uses and Disclosures

Disclosures required by law (continued)

— For Example:

• Nearly every state has mandatory reporting requirements related to injuries caused by firearms or other dangerous weapons.

• Many states have mandatory reporting requirements related to child abuse, elder abuse, domestic violence, and sexual assault.

— Remember – This requirement is limited to the information that is required to be reported.

• Typically does not include photographs.
Permitted Uses and Disclosures

Victims of Abuse, Neglect or Domestic Violence

• May disclose PHI about an individual whom you reasonably believe to be a victim of abuse, neglect, or domestic violence to an authorized government authority, if:
  – the disclosure is required by law;
  – the individual agrees to the disclosure; or
  • oral consent satisfies this requirement
  – the disclosure is expressly authorized by legislation, and
    • necessary to prevent serious injury; or
    • where the individual is unable to agree because of incapacity and a law enforcement official represents that the information is not intended to be used against the individual and that an immediate enforcement activity depends on the disclosure . . .
Permitted Uses and Disclosures

Victims of Abuse, Neglect or Domestic Violence

• You must inform the individual of the disclosure when disclosure is made to a government authority as required by law, and the victim has not specifically provided consent for the disclosure, unless
  – informing the individual would place her or him in serious harm; or
  – would require informing a personal representative who you believe is responsible for the abuse, neglect or harm.
Permitted Uses and Disclosures

Disclosures for judicial and administrative proceedings

• May disclose PHI
  – In response to a court order
  – In response to a subpoena; if
    • The individual has been given notice of the request; and
    • The requestor has made sufficient efforts to obtain a protective order protecting the information.
Permitted Uses and Disclosures

Disclosures for law enforcement purposes

• May disclose PHI:
  – As required by laws that require the reporting of certain types of injuries.
  – In compliance with a court order, warrant, subpoena, summons, grand jury subpoena, or administrative request.
  – Information related to the victim of a crime, in response to law enforcement request
    • with consent of the victim;
    • if unable to obtain consent because of incapacity with necessary assurances from law enforcement.
  • If the individual is the victim of abuse, neglect or domestic violence, you must follow the specific reporting requirement related to such offenses.
Permitted Uses and Disclosures

Disclosures to for law enforcement purposes (continued)

• When providing emergency care, a health care provider may disclose PHI to a law enforcement official if such disclosure is necessary to alert law enforcement to:
  – the commission and nature of a crime;
  – the location of such crime; and
  – the identity, description and location of the perpetrator.
Permitted Uses and Disclosures

2. Disclosures for which the opportunity to agree or object is required
   a. Disclosure for facility directories
      • May disclose the individual’s name, location in the facility, a general description of their condition, and their religious affiliation.
      • Individual must be informed in advance of the disclosure, including the information to be disclosed and the persons to whom the information may be disclosed,
      • Individual must be given an opportunity to refuse or otherwise restrict the disclosure
Permitted Uses and Disclosures

2. **Disclosures for which the opportunity to agree or object is required**
   
b. **Disclosure for involvement in the individuals care and notification purposes**
   
   • May disclose to a family member, relative, friend, or other person identified by the individual, information related to the person’s involvement in the patient’s care or payment related to the patient’s care.
   
   • May disclose information including the patient’s name, location, general condition, or death to notify a family member, personal representative or other person responsible for the patient’s care.
   
   • Individual must be given an opportunity to refuse or otherwise restrict the disclosure (may be inferred from the circumstances).
Permitted Uses and Disclosures

3. Uses and disclosures for which authorization is required.
   a. Except as other permitted by HIPAA.
   b. Authorization for use or disclosure of psychotherapy notes is required, notwithstanding any other provisions, except:
      - use by the originator of the notes;
      - training of the covered entity’s own students, trainees or practitioners in mental health;
      - by covered entity to defend itself in litigation brought by the individual.
   c. Authorization required for use in Marketing, with limited exceptions.
## HIPAA Disclosures Summary

<table>
<thead>
<tr>
<th>Disclosure Required</th>
<th>Without Authorization</th>
<th>Opportunity to Object</th>
<th>With Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Upon request by the individual who is the subject of the information</td>
<td>1. Treatment, Payment, Operations</td>
<td>1. Facility Directories</td>
<td>1. Except as otherwise permitted</td>
</tr>
<tr>
<td>2. To HHS for compliance investigation, review, or enforcement action</td>
<td>2. Required by Law</td>
<td>2. Individual Care or Notification Purposes</td>
<td>2. Authorization required for disclosure of psychotherapy notes</td>
</tr>
<tr>
<td></td>
<td>3. Abuse, Neglect, Domestic Violence • required by law • with consent</td>
<td></td>
<td>3. Authorization required for use in marketing</td>
</tr>
<tr>
<td></td>
<td>4. In response to a Court Order or Subpoena</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Law Enforcement Purposes: • as required by law • with Consent • Subpoena/court order • In emergency</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Valid Authorization

Core Elements – Authorization must contain:

• A description of the information to be used or disclosed
• The name or other identifying information of the person authorized to make the requested use or disclosure
• The name or other identifying information of the person to whom the entity may make the disclosure
• A description of each purpose of the requested use or disclosure
• An expiration date or event
• Signature of the individual and date
Valid Authorization

Required Statements.

• In addition to the Core Elements, the Authorization must contain statements adequate to put the individual on notice of:
  – The individual’s right to revoke the authorization in writing including how the individual may revoke the authorizations and the exceptions to the right to revoke;
  – The ability or inability to condition treatment on the authorization (providers may condition treatment on authorization only in very limited circumstances).
  – The potential for the information to be re-disclosed by the recipient and no longer be protected.
Valid Authorization

- The authorization must be written in plain language.
- The covered entity must provide a copy of the signed authorization to the individual.
Valid Authorization

Defective Authorizations:

• The expiration date has passed;
• Core elements are incomplete;
• Authorization has been revoked;
• The covered entity knows that material information is false.
Valid Authorization

Compound Authorizations:

• Generally, the authorization may not be combined with any other document to create a compound authorization.
Valid Authorization

Prohibition on Conditioning of Authorizations.

• A covered entity generally may not condition the provision of treatment on the provision of an authorization.

• Exceptions:
  – Research-related treatment;
  – Health care that is solely for the purpose of creating protected health information for disclosure to a third party.
HIPAA Security Rule

• What information is covered by the Security Rule?
  – “Electronic Protected Health Information” ("e-PHI").
  – e-PHI includes all individually identifiable health information that a covered entity creates, receives, maintains or transmits in electronic form.
  – Unlike the Privacy Rule, the Security Rule does not apply to PHI transmitted orally or in writing.
HIPAA Security Rule

- Requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguard for e-PHI.
- Specifically, covered entities must:
  1. Ensure the confidentiality, integrity, and availability of all e-PHI
  2. Identify and protect against reasonably anticipated threats to security or integrity of the information;
  3. Protect against reasonably anticipated, impermissible uses or disclosures; and
  4. Ensure compliance by their workforce.
HIPAA Security Rule

• **Confidentiality** = Not available or disclosed to unauthorized persons.

• **Integrity** = Not altered or destroyed in an unauthorized manner.

• **Availability** = Accessible on demand to authorized persons.
HIPAA Security Rule

• Administrative Safeguards

• Physical Safeguards

• Technical Safeguards
Administrative Safeguards

• Security Management Process – Must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities accordingly.

• Security Personnel – Must designate a security official who is responsible for developing and implementing its security policies and procedures.

• Information Access Management – Must develop policies and procedures for authorizing access to e-PHI only when access is appropriate.

• Evaluation – Must perform periodic assessments.
Physical Safeguards

• Facility Access and Control - Must limit physical access while ensuring authorized access is allowed.

• Work Station Device Security
  – Requires policies and procedures governing use and access to work stations and electronic media.
  – Must have P&Ps regarding transfer, removal, disposal, and re-use of electronic media.
Technical Safeguards

- **Access Controls** – Technical P&Ps that allow only authorized access to e-PHI.
- **Audit Controls** – Hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- **Integrity Controls** – P&Ps to ensure that e-PHI is not improperly altered or destroyed.
- **Transmission Security** – Technical security measures that guard against the unauthorized access to e-PHI that is being transmitted over an electronic network.
HIPAA Security Rule

• Covered entities must comply with every Security Rule Standard.
• Each Security Rule Standard contains both “Required” and “Addressable” implementation specifications.
  – Required Implementation Specifications must be implemented
  – Addressable Implementation Specifications
    • Not optional
    • Covered entities may determine whether the specification is reasonable and appropriate for that entity.
### Administrative Safeguards

<table>
<thead>
<tr>
<th>Required Specifications</th>
<th>Addressable Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Risk Management/Analysis</td>
<td>• Malicious Software Protection</td>
</tr>
<tr>
<td>• Sanction Policy</td>
<td>• Log-in Monitoring</td>
</tr>
<tr>
<td>• Data Backup/Recovery Plans</td>
<td>• Password Management</td>
</tr>
</tbody>
</table>

### Physical Safeguards

<table>
<thead>
<tr>
<th>Required Specifications</th>
<th>Addressable Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Disposal</td>
<td>• Maintenance Records</td>
</tr>
<tr>
<td>• Media Reuse</td>
<td>• Data Backup and Storage</td>
</tr>
</tbody>
</table>

### Technical Safeguards

<table>
<thead>
<tr>
<th>Required Specifications</th>
<th>Addressable Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unique User ID</td>
<td>• Encryption</td>
</tr>
<tr>
<td>• Emergency Access Procedure</td>
<td></td>
</tr>
</tbody>
</table>
HIPAA Security Rule

• Covered entities range from the smallest health care provider to the largest multi-state health plan.
  – Have very different security needs
  – The Security Rule is intended to be flexible

• Considerations in developing Security Measures
  – Size, complexity, and capabilities
  – Technical, hardware, and software infrastructure,
  – The costs of security measures, and
  – The likelihood and possible impact of potential risks to e-PHI.

• Must review and modify security measures to continue protecting e-PHI in a changing environment.
HITECH

• The Health Information Technology for Economic and Clinical Health ("HITECH") Act
  • Enacted as part of the American Recovery and Reinvestment Act of 2009.
  • Requires covered entities to notify individuals of unauthorized disclosures of unsecured PHI.
  • Breach notification requirements are not triggered if information is rendered unreadable through encryption.
  • Substantially increased sanctions for HIPAA violations.
State Laws
State Health Information Privacy

• All states have health information privacy laws that supplement HIPAA.
• State laws cannot relieve Covered Entities from HIPAA obligations.
• State laws can and do impose more stringent requirements.
• State laws frequently impose privacy requirements on providers and other entities that are not “covered entities” under HIPAA.
State Health Information Privacy

• Property rights over medical records and their contents are determined by state law.
  – In most states, including California, the Medical Record belongs to the provider.
  – Patients have a right to a copy, but not the original.
  – Once something is put into the medical record, it is the property of the provider.
    • This includes information and images from forensic exams.
State Health Information Privacy

• Other state laws that do not specifically govern health information privacy, supplement and clarify HIPAA obligations.
• For example, state laws imposing reporting requirements on health care providers and other professionals clarify circumstances under which PHI may be disclosed.
State Health Information Privacy

• Every state has laws imposing obligations on health care providers to report treatment related certain injuries and conditions to law enforcement or other state officials.

• As discussed, under HIPAA, health care providers may disclose PHI to law enforcement and other authorized government officials, without the consent or authorization of patients, where disclosure is part of a report required by law.
State Reporting Requirements

• Many states have laws requiring health care providers to report known or reasonably suspected cases of rape, sexual assault or abuse.
State Reporting Requirements

- State reporting requirements regarding sexual assault of adults typically fall into four categories:
  1. State laws that require providers to report treatment related to rape, sexual assault or domestic violence.
  2. State laws that require providers to report treatment related to intentional or non-accidental injuries.
  3. State laws that require providers to report treatment related to injuries caused by criminal acts, including rape, sexual assault or domestic violence.
  4. State laws that require reporting of treatment related to injuries caused by fire arms or other dangerous weapons.
Sexual Assault Reporting Requirements

- Red (Massachusetts) – Must Report Rape or Sexual Assault (but may not identify victim)
- Blue (California) – Must Report sexual battery, including assault with intent to commit rape.
- Green (Kentucky) – Must report incidents of spousal rape.
Intentional Injury Reporting Requirements

- Red – Must Report Intentional Injuries (if the injury is likely to cause death).
- Blue – Must Report Intentional Injuries.
- Green – Must Report Intentional Injuries (except for domestic violence unless serious bodily injury or caused by a deadly weapon).
Reporting Requirements for Injuries Caused by Criminal Acts

- Red – Must Report Injuries Caused by Criminal Conduct (but may not identify rape or sexual assault victims)
- Blue – Must Report Injuries Caused by Criminal Conduct
- Green – Must Report Injuries Caused by Criminal Conduct (except for domestic violence).
Reporting Requirements for Injuries Caused by Deadly Weapons

- Mandatory Reporting
- No Mandatory Report
State Reporting Requirements

• California Law requires Health Care Practitioner to:
  1. Immediately, or as soon as possible, make a report by telephone to local law enforcement; and
  2. Prepare a written report to send to local law enforcement within two working days of receiving the information. The written report must include:
     • The name of the injured person, if known;
     • The injured person’s whereabouts;
     • The character and extent of the persons injuries;
     • The identity of any person the injured person alleges inflicted the wound, other injury, or abusive conduct upon the person.
State Reporting Requirements

• All states have laws requiring health care providers to report known or reasonably suspected cases of child abuse or neglect.
• Most states have laws requiring health care providers to report known or reasonably suspected cases of elder abuse to either law enforcement or State Adult Protective Services.
Elder Abuse Reporting Requirements

- Must Report
- May Report
- No Law
Informed Consent
Informed Consent

• Two separate and distinct consent process: One for medical treatment and one for the forensic examination.
• A third consent may be required for use and disclosure under HIPAA.
• Patients should be informed of applicable state law reporting requirements as part of the informed consent for the forensic examination.
Informed Consent

• Patients should understand the full nature of their consent to each procedure, including, for example, what the procedure entails, possible side effects, and potential impact.
• Patients can decline any part or all of treatment or the examination.
• Informing patients of the potential affect of declining a particular procedure is part of the informed consent process.
• Failure to obtain appropriate informed consent, including failure to inform the patient of the potential affect of declining a procedure, may be malpractice.
Informed Consent

• [T]he informed consent process includes making patients aware of the impact of declining a procedure, as it may negatively affect the quality of care and the usefulness of the evidence collection. It may also have a negative impact on a criminal investigation and/or prosecution both because evidence collected may have been useful and because defense attorneys may use the fact that the victim declined a procedure to claim that the victim is hiding something that would have been revealed by that procedure.\(^\text{12}\)
Informed Consent

• When informed consent is required, and when informed consent is effective, is determined by state law, and thus varies between states.
• Generally, informed consent is necessary for medical evaluation and treatment related to the following:
  – General medical care;
  – Pregnancy testing and care;
  – Testing and prophylaxis for STIs;
  – HIV prophylaxis;
  – Permission to re-contact the patient for medical purposes; and
  – Release of medical information.
Informed Consent

- Informed consent is generally necessary for the forensic exam and evidence collection for:
  - Notification to law enforcement or other authority (depending on reporting requirements);
  - Photographs;
  - The examination itself and evidence collection;
  - Toxicology screening;
  - Release of information and evidence to law enforcement;
  - Permission to contact patients;
  - Patient notification in case of DNA match or additional victims.
Informed Consent

• An effective “informed consent” necessarily requires an understanding of the nature and purpose of proposed and alternative treatments.

• If patients are unable to understand the risks and benefits of proposed and alternative treatments, they are incompetent to give effective consent.
Informed Consent

• In California, competency for purposes of consent for medical treatment is defined as “the ability to understand the nature and consequences of the illness, the proposed treatment, alternatives to treatment, and the ability to make a reasoned decision in this regard.”

• Patients may be considered temporarily incompetent to give consent for many reasons including: incapacitating injuries, sedation, intoxication, etc.

• Competency is a case-by-case determination. Your institution should designate someone to be consulted in instances where competency to consent becomes an issue.
Informed Consent vs. Authorization to Disclose

• Can an authorization to disclose under HIPAA be combined with informed consent.
  – Compound authorizations are defective under HIPAA.
  – However, HIPAA does not require an “authorization” to disclose information related to victims abuse, neglect, and domestic violence or victims of a crime.
Informed Consent vs. Authorization to Disclose

• Remember - a covered entity may disclose PHI about a victim of abuse neglect, or domestic violence to an authorized government authority, if:
  – the disclosure is required by law, or
  – the individual agrees to the disclosure.
    • May be oral.
    • may be combined with other consents except as prohibited by state law.
Informed Consent vs. Authorization to Disclose

• Similarly, an entity may disclose PHI about a victim of a crime to a government authority for law enforcement purposes:
  – If the disclosure is required by law, or
  – With the consent of the victim in response to a law enforcement request.
    • May be oral.
    • May be combined with other consents except as prohibited by state law.
News Release

FOR IMMEDIATE RELEASE
Tuesday, February 22, 2011

HHS imposes a $4.3 million civil money penalty for violations of the HIPAA Privacy Rule.

Action marks first civil money penalty issued by HHS for HIPAA Privacy Rule violations.

The U.S. Department of Health and Human Services’ (HHS) Office for Civil Rights (OCR) has issued a Notice of Final Determination finding that Cigna Health of Prince George’s County, Md., (Cigna) violated the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HHS has imposed a civil monetary penalty (CMP) of $4.3 million for the violations, representing the first CMP issued by the Department for a covered entity’s violations of the HIPAA Privacy Rule.

The CMP is based on the violation categories and increased penalty amounts authorized by Section 13410(d) of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

“Ensuring that Americans’ health information privacy is protected is vital to our health care system and a priority of this Administration. The U.S. Department of Health and Human Services is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule,” said HHS Secretary Kathleen Sebelius.
Increased HIPAA Enforcement


- HHS imposed $4.3 Million Civil Monetary Penalty against Cignet Health for violations of the HIPAA Privacy Rule.
  - $1.3 Million for denying patients access to the medical records.
  - $3 Million for failing to cooperate with the investigation.
- First time that the Federal Government has imposed CMPs for HIPAA Privacy Rule violations.
Increased HIPAA Enforcement

• Covered entities . . . must uphold their responsibility to provide patients with access to their medical records, and adhere closely to all of HIPAA’s requirements. The U.S. Department of Health and Human Services will continue to investigate and take action against those organizations that knowingly disregard their obligations under these rules.

— OCR Director Georgina Verdugo
Increased HIPAA Enforcement

News Release

FOR IMMEDIATE RELEASE
Thursday, February 24, 2011

Massachusetts General Hospital settles potential HIPAA violations

Large hospital system to improve policies and procedures safeguarding patient information

The General Hospital Corporation and Massachusetts General Physicians Organization Inc. (Mass General) has agreed to pay the U.S. government $1,000,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, the U.S. Department of Health and Human Services (HHS) announced today.

Mass General, one of the nation’s oldest and largest hospitals, signed a Resolution Agreement with HHS that requires it to develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients. The settlement follows an extensive investigation by the HHS Office for Civil Rights (OCR), which enforces the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule requires health plans, health care clearinghouses and most health care providers (covered entities) to protect the privacy of patient information through administrative, physical and technical safeguards at all times.

"We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity’s responsibility to protect its patients’ health information," said OCR Director Georgina Verdugo.
Increased HIPAA Enforcement

Massachusetts General Hospital. (Feb. 24, 2011).

• Agreed to pay $1 Million to resolve allegations related to “potential violations” of HIPAA related to 192 patient medical records lost by an employee on a subway on the way to work.

• OCR’s investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General’s premises and impermissibly disclosed PHI potentially violating provisions of the HIPAA Privacy Rule.

• As part of the resolution, Mass General agreed to develop new policies with respect to physical removal and transport of PHI from hospital premises, laptop encryption, and USB drive encryption.
Increased HIPAA Enforcement

• We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity’s responsibility to protect its patients’ health information.

– OCR Director Georgina Verdugo
Increased HIPAA Enforcement

• Lessons
  – The Government is getting serious about HIPAA enforcement.
  – Must continuously review and modify policies and measures that can be used to protect PHI, particularly e-PHI that is susceptible to loss or other unauthorized disclosure.
To Encrypt Or Not To Encrypt?
Encryption

- Do I have to encrypt data?
  - It depends

- Encryption is an addressable specification, not a required specification
  - Is encryption reasonable and appropriate under the circumstances?
Encryption

- Considerations in developing security measures
  - Size, complexity, and capabilities
  - Technical, hardware, and software infrastructure,
  - The costs of security measures, and
  - The likelihood and possible impact of potential risks to e-PHI.
Encryption

CMS HIPAA Security Guidance for Remote Use of and Access to e-PHI

- [Recommends that covered entities] require that all portable or remote devices that store EPHI employ encryption technologies of the appropriate strength . . . Because of the proliferation of portable devices and media, the risk of loss or theft of ePHI has increased.

- Although this implementation specification is addressable, strong encryption provides additional assurances over the protection of ePHI, even in cases where portable devices are lost or stolen.

- The combination of CMS’s recommendation in the remote use guidance, the increasing number of incidents involving lost portable devices, and the decreasing cost of encryption solutions has resulted in an environment where encryption may not be optional under the mantra of reasonable and appropriate.
Encryption

• Though “addressable,” encryption is “recommended”
  – CMS in its HIPAA Security Guidance for Remote Use of and Access to e-PHI.

• In the event of a breach, lack of encryption may be deemed a failure to implement reasonable and appropriate safeguards to protect e-PHI.
  – Mass General enforcement action and settlement

• HITECH, if data is encrypted, breach notification is not required.
Whose Record Is It Anyway?
Whose Record Is It?

- In California, and most other states, the medical record, and its contents generally belongs to the provider.
- Once the forensic examination is completed and put into the medical record it belongs to the provider.
- How about before it is physically placed in the medical record?
Whose Record Is It?

• Very little law on the issue.
• It may depend on:
  – Where the examination was conducted;
  – Who conducted the exam;
  – What the patient was told during the informed consent;
• Were they told the examination was for medical treatment purposes, evidentiary purposes, or both.
Whose Record Is It?

- In absence of state law or other definitive resolution, HIPAA covered entities must protect the record and seek the consent of the victim before disclosing the record to law enforcement.
References


5. Source: Teresa P. Scalzo, Esq.; SUMMARY OF LAWS RELEVANT TO RAPE AND SEXUAL ASSAULT REPORTING FOR THE VICTIMIZATION OF COMPETENT ADULTS; available at http://www.usmc-mccs.org/famadv/restrictedreporting/National%20Rape%20Reporting%20Requirements%206.15.06.pdf.


7. Source: Teresa P. Scalzo, Esq.; SUMMARY OF LAWS RELEVANT TO RAPE AND SEXUAL ASSAULT REPORTING FOR THE VICTIMIZATION OF COMPETENT ADULTS; available at http://www.usmc-mccs.org/famadv/restrictedreporting/National%20Rape%20Reporting%20Requirements%206.15.06.pdf.

8. Source: Teresa P. Scalzo, Esq.; SUMMARY OF LAWS RELEVANT TO RAPE AND SEXUAL ASSAULT REPORTING FOR THE VICTIMIZATION OF COMPETENT ADULTS; available at http://www.usmc-mccs.org/famadv/restrictedreporting/National%20Rape%20Reporting%20Requirements%206.15.06.pdf.

9. Source: COMPARISON CHART OF PROVISIONS IN ADULT PROTECTIVE SERVICES LAWS, BY STATE (Laws current as of 12/31/06); Prepared by Lori Stiegel and Ellen Klem of the American Bar Association Commission on Law and Aging for the National Center on Elder Abuse; available at http://www.americanbar.org/groups/law_aging.html.
References

12. Id.
16. CENTERS FOR MEDICARE & MEDICAID SERVICES; HIPAA SECURITY GUIDANCE FOR REMOTE USE OF AND ACCESS TO ELECTRONIC PROTECTED HEALTH INFORMATION.