I. The differing roles, responsibilities, legal authority, and objectives of law enforcement and health care providers

A. Health Care Providers: Protect and promote the health of patients and public

1. Wisconsin Definition of “Health care provider” – includes nurses, physicians, practice groups, hospices, inpatient health care facilities, CBRFs, and rural medical centers. (Wis. Stat. § 146.81)

2. Federal and state privacy laws provide for the confidentiality of patient information, and create legal responsibilities for health care providers to maintain that confidentiality.

B. Law Enforcement: Enforce the law and promote public safety

1. Legal definitions under Wisconsin law

   a) “Law enforcement officer” – any person employed by the state or any political subdivision of the state for the purpose of detecting and preventing crime and enforcing laws or ordinances and who is authorized to make arrests for violations of the laws or ordinances that the person is employed to enforce (Wis. Stat. §§ 165.85, 175.46) OR any person who by virtue of the person’s office or public employment is vested by law with the duty to maintain public order or to make arrests for crimes while acting within the scope of the person’s authority (Wis. Stat. § 967.02)

   b) “Law enforcement agency” – a governmental unit of one or more persons employed full time by the state or a political subdivision of the state for the purpose of preventing and detecting crime and enforcing state laws or local ordinances, employees of which unit are authorized to make arrests for crimes while acting within the scope of their authority. (Wis. Stat. § 165.83)

2. HIPAA definition of “Law enforcement official” An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

   a) Investigate or conduct an official inquiry into a potential violation of law; or
b) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

3. HIPAA does not apply to law enforcement agencies or officers, because they are neither a covered entity nor a business associate. Nonetheless, information they receive may be protected under state privacy laws, including Wis. Stat. § 146.82.

4. Law enforcement officers will be concerned about constitutional limits on gathering information, such as prohibitions against unreasonable searches and seizures and their obligations under the Due Process Clause.

II. Privacy laws should be considered

The privacy of health care information is protected by both federal and state laws. There are penalties for non-compliance with privacy law, including forfeitures, criminal penalties, civil litigation and negative public relations or loss of patient trust.

A. Federal Laws

1. HIPAA – Health Insurance Portability and Accountability Act of 1996

   a) What is HIPAA?

      (1) Established during the Clinton administration, HIPAA privacy was the first enforceable, federally-mandated, comprehensive set of privacy rights and responsibilities. It became effective in 2001.

      (2) Established in order to improve productivity of the health care system and protect the privacy and security of health information.

      (3) Sets the standards (electronic and physical security) for the security of health care data while stored or transmitted.

   b) What does HIPAA do?

      (1) HIPAA protects the privacy and security of a patient’s health information.

      (2) Prevents health care fraud and abuse – created the Health Care Fraud and Abuse Control Program.

      (3) Protects rights to health insurance coverage when changing jobs, losing a job, getting divorced, or becoming pregnant.

      (4) Administrative simplification – reduces costs and administrative burdens of health care by standardizing the electronic transmission of administrative/financial transactions.
c) HIPAA Basics

(1) “Covered Entity” – 3 basic groups of individuals/corporate entities:

(a) Health Care Provider – provider of medical or health services, and entities who furnish, bill, or are paid for health care in the normal course of business.

(b) Health Plan – any individual or group that provides or pays for the cost of medical care, including employee benefit plans.

(c) Healthcare Clearinghouse – any entity that either processes or facilitates the processing of health information.

(2) “Protected Health Information”

(a) What is PHI? Name, address (geographic subdivisions smaller than a state), email address, dates (except years) including admission/discharge and birth date, phone numbers, fax numbers, SSN, medical record number, health plan beneficiary number, account number, certificate/license numbers, VIN, license plate numbers, device identifiers and serial numbers, URLs, IP address, biometric identifiers, full face photographic images, any other unique identifier or code.

(b) PHI is covered by HIPAA when you use it, disclose it, store it, see it on your computer, when it is lying on your desk, when you share it with another health care provider, or a contracted service provider, and when you talk about it face to face and over the phone.

(c) PHI is not subject to HIPAA regulations when it is de-identified. PHI is de-identified:

(i) By removing identifiers (all 18 elements) and there is no reasonable basis that an individual can be identified

(ii) By eliminating, concealing, or completely redacting

(iii) By obtaining a statistician certification that the data is de-identified

(3) “Individually Identifiable Information”

(a) Any information, including demographic information collected from an individual that:

(i) is created or received by a covered entity; and
(ii) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment of the provision of health care to an individual; and

(a) identifies the individual or

(b) with respect to whether there is a reasonable basis to believe that the information can be used to identify the individual

(4) “Minimum necessary” standard – a covered entity must make reasonable efforts to limit the use or disclosure of, and requests for PHI, to a minimum amount necessary to accomplish the intended purpose.

(5) Use vs. disclosure of PHI

(a) Use – the sharing, employment, application, utilization, examination or analysis of PHI within the covered health care component that maintains the PHI

(b) Disclosure – release, transfer, provision of access to, or divulging in any other manner of PHI outside the covered health care component holding the PHI

(6) Permitted Uses and Disclosures

(a) Treatment, Payment and Health Care Operations – PHI may be used and/or disclosed without a patient’s authorization for purposes of treatment, payment, or health care operations

(i) Treatment

(a) Provision, coordination or management of health care and related services by a health care provider

(b) Coordination and management of health care by a health care provider with a third party (e.g. HMO)

(c) Consultations among providers
(ii) Payment

(a) Activities by a health plan to obtain premiums or fulfills obligations for coverage and the provision of benefits (e.g., eligibility)

(b) Activities by either a provider or health plan to obtain or provide reimbursement.

(iii) Health Care Operations

(a) Support treatment and payment activities. e.g.: quality improvement, legal and audit services, business planning, general administration

(b) Operations are limited to the covered entity’s operations – not the operations of law enforcement.

(b) Permitted use and disclosure as required by law

(i) e.g., court order, court-ordered warrant, subpoena or summons issued by a judicial officer, grand jury subpoena, administrative subpoena, summons, investigative demand

(a) Provided that:

(i) The information sought must be relevant and material to a legitimate law enforcement inquiry.

(ii) The request must be specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

(iii) De-identified information could not reasonably be used

(b) Does not include a subpoena from a lawyer.

(ii) Permitted use and disclosure to law enforcement (following both state law and HIPAA) and other permitted uses and disclosures:

(iii) Adult abuse, neglect, or domestic violence
(iv) Child abuse or neglect

(v) Judicial and administrative proceedings (following both HIPAA and state law)

(vi) Avert serious threat to health or safety

(vii) Public health activities

(viii) Information for identification and location of suspect, fugitive, material witness, or missing person, limited to: name; address; date and place of birth; SSN; ABO blood type and Rh factor; type of injury; date and time of treatment; date and time of death; and description of distinguishing physical characteristics including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

(7) When are authorizations needed?

(a) For disclosure of PHI for purposes other than treatment, payment or health care operations or that are not otherwise allowed under regulations.

(b) To disclose psychotherapy notes.

(c) For marketing purposes.

(8) Breach

(a) An unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information, except when an unauthorized person to whom such information is disclosed would not reasonably be expected to be able to retain such information.

(b) Disclosing PHI to someone who did not have the authority to receive it is a breach.

2. HITECH – Health Information Technology Economic and Clinical Act

a) What is HITECH?

(1) Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) which made significant changes to HIPAA privacy and security regulations.

(2) Part of the federal government’s plan to increase adoption and use of health information technology and health information exchanges. Effective 2/17/2009
b) What does HITECH do?
   
   (1) Increased funding and protections to respond to increased adoption and use of health information technology. $33 billion in incentives to providers who utilize electronic health records

   (2) Requires notification of a breach to U.S. Department of Health & Human Services and affected individuals. Prior to HITECH, there was no affirmative obligation to notify individuals or the HHS of a breach of Privacy or Security Rules. Rather, the covered entity had an obligation to mitigate any harm caused by the breach, which may have included notification.

c) HITECH breach notification requirements became effective September 2009.

d) The Final HITECH Rule was released on January 17, 2013 and became effective on March 26, 2013. Compliance with the Final HITECH Rule was required by September 23, 2013.

B. Wisconsin law

1. General

   a) Wisconsin has enjoyed strong confidentiality laws for many years, even when other states (and the federal government) had less stringent laws.

   b) HIPAA did not replace state confidentiality laws – it acts as a floor—establishing the minimum protections of privacy protection. More stringent state laws, regulations, or policies prevail over the less protective HIPAA requirements.

2. Confidentiality of Patient Health Care Records  Wis. Stat. § 146.82

   a) All patient health records shall remain confidential and may only be released with the consent of the patient or as authorized under state law or HIPAA (45 CFR 164, subpart E).

   b) Disclosures to law enforcement may be made under the following circumstances:

      (1) Under a lawful order of a court of record;

      (2) To an elder-adult-at-risk agency or adult-at-risk agency;

      (3) For purposes of reporting, investigating, or prosecuting threatened or suspected child abuse or neglect;

      (4) For purposes of investigating certain deaths;

      (5) Related to prisoners or persons in custody, as appropriate; or
The information is requested for a ch. 980 proceeding (the civil commitment of sexually violent persons).

c) An entity that receives this information may only redisclose the information if (1) authorized by the patient; (2) ordered by the court; or (3) the redisclosure is limited to the purpose for which the patient health care record was initially received.

3. Mental Health Records Wis. Stat. § 51.30

a) Covers records created in the course of providing treatment for mental illness, alcoholism, drug dependence, or developmental disabilities.

b) Disclosure of records protected under § 51.30 is more limited than for other health care records.

c) May be disclosed to law enforcement under the following circumstances:

(1) there is informed consent of the patient, or the person who is legally authorized to give consent for the patient;

(2) there is a lawful order of a court of record;

(3) the information is requested for a ch. 980 proceeding (the civil commitment of sexually violent persons);

(4) a civilly committed patient has eloped;

(5) the Department of Health Services authorizes disclosure of certain information about civilly a committed individual;

(6) to report or provide information on child abuse or neglect;

(7) to report an apparent crime on the premises; or

(8) to report certain deaths.

d) The unlawful disclosure of information may result in fines up to $25,000 and imprisonment for up to 9 months.

e) The Department of Health Services has promulgated Administrative Code, chapter DHS 92, to implement this section.

4. Restrictions on the Use of HIV Tests Wis. Stat. § 252.15

a) HIV status may be shared:

(1) to permit a jailer or prison officials to add to medical record or to assign a private cell;
(2) when certain persons have had significant exposure to body fluid, as outlined under (5g).

b) Penalties for violating this provision include fines of up to $50,000 and imprisonment of up to 9 months.

III. Mandatory and permissive reporting laws

A. Mandatory Reporting


a) Requires reporting when the provider “has reasonable cause to suspect that a child seen by the person in the course of professional duties has been abused or neglected or who has reason to believe that a child seen by the person in the course of professional duties has been threatened with abuse or neglect and that abuse or neglect of the child will occur”

b) Requires reporting when the provider has reason to suspect than an unborn child “has been abused” or “is at substantial risk of abuse.” In order to substantiate that unborn child abuse has occurred, the child welfare worker must have information that establishes the following: (1) pregnant woman habitually lacks self-control in the use of alcohol beverages, controlled substances, or controlled substance analogs, exhibited to a severe degree; (2) there is a substantial risk to the physical health of the unborn child; and (3) the child when born will be seriously affected or endangered unless the woman receives prompt and adequate treatment.

c) Providers are not necessarily required to report all instances of adolescent sexual contact or intercourse. Wis. Stat. § 48.981(2m)

d) Persons who fail to report suspected child abuse when required may be fined not more than $1,000 or imprisoned not more than six months or both.

2. Elder Adults at Risk, Wis. Stat. § 46.90(4) and Adults at Risk, Wis. Stat § 55.043(1m)

a) Except when it would not be in the best interest of the person, a health care provider who has seen an adult at risk in the course of the person's professional duties shall file a report with the appropriate agency or local law enforcement, if the adult at risk has requested the person to make the report, or if the person has reasonable cause to believe that any of the following situations exist:

(1) The adult at risk is at imminent risk of serious bodily harm, death, sexual assault, or significant property loss and is unable to make an informed judgment about whether to report the risk.
(2) An adult at risk other than the subject of the report is at risk of serious bodily harm, death, sexual assault, or significant property loss inflicted by a suspected perpetrator.

b) Any person making a report is presumed to make it in good faith.

3. Gunshots, Burns, Wounds Resulting from a Crime Wis. Stat. § 255.40(2)

a) Requires reporting of:

(1) A gunshot wound.

(2) Any wound other than a gunshot wound if the person has reasonable cause to believe that the wound occurred as a result of a crime.

(3) Second-degree or 3rd-degree burns to at least 5% of the patient's body or, due to the inhalation of superheated air, swelling of the patient's larynx or a burn to the patient's upper respiratory tract, if the person has reasonable cause to believe that the burn occurred as a result of a crime.

b) For any mandatory report the person shall report the patient's name and the type of wound or burn injury involved as soon as reasonably possible to the local police department or county sheriff's office for the area where the treatment is rendered.

c) Intentionally failure to report subject to forfeiture of not more than $500.

d) Any person reporting in good faith and any inpatient health care facility that employs the person who reports, are immune from all civil and criminal liability that may result because of the report. In any proceeding, the good faith of any person reporting under this section shall be presumed.

e) The reporting requirement under sub. (2) does not apply under any of the following circumstances:

(1) The patient is accompanied by a law enforcement officer at the time treatment is rendered.

(2) The patient's name and type of wound or burn injury have been previously reported.

(3) The gunshot wound appears to have occurred at least 30 days prior to the time of treatment.

B. Permissive Reporting

4. Crimes on premises, 45 CFR 164.512(f)(5)
5. Correctional institutions and other law enforcement custodial situations, 45 CFR 164.512(k)(5)

6. To avert a serious threat to health or safety, 45 CFR 164.512(j)

7. Other permissive reporting statutes

IV. Police Practices Impacting Privacy

A. Body Cameras

1. Purpose: To provide a truer record of a police/suspect contact than individual recollections. The camera memorializes the contact, with the goal of making police officer actions more transparent and police officers and departments more accountable. Use of the cameras also captures evidence and may insulate officers and departments from false claims of abuse or violations of rights.

2. Use: Use of body cameras by police departments appear to be here to stay. More and more Wisconsin police departments are using cameras or are planning to use them. The hope is that body cameras will serve and protect both the police and the public.

3. Privacy Issues: There is little dispute about the virtues of a body camera system for the police. But they do raise collateral problems such as privacy issues in a hospital. It is best to address these issues in the quiet of a proactive planning meeting than in the din of an ongoing police/suspect contact.

B. Body Cavity Searches

1. Wis. Stat. § 968.255 (3) provides that only a physician, physician assistant, or registered nurse may perform a body cavity search.

2. There typically is no problem if the subject consents to the search. But if the subject does not consent the police can still ask for a body cavity search, if they have probable cause to do so.

3. Hospitals have been reluctant to perform these body cavity searches without some kind of court order. Many hospitals were reluctant to perform a body cavity search to a resistant suspect, even with a search warrant, because of liability and risk management concerns. The legislature responded to this concern by enacting 2015 Wisconsin Act 238. This law, which became effective March 3, 2016, grants immunity to a physician, physician assistant, and/or registered nurse, who conducts the body cavity search. The protection of immunity extends to their employer and the hospital where the search is performed. This new law is codified at Wis. § 895.535, and referenced at Wis. Stat. § 968.255(3).
C. Tests for Intoxication

1. Wisconsin has an implied consent law, whereby any person who is on duty time with respect to a commercial motor vehicle or operates a motor vehicle is deemed to have given consent to one or more tests of his or her breath, blood, or urine, for the purpose of determining the presence or quantity in his or her blood or breath, of alcohol, controlled substances, controlled substance analogs or other drugs, or any combination of these, when requested to do so by a law enforcement officer. Any such tests shall be administered upon the request of a law enforcement officer. Persons who are unconscious have not revoked this consent. Persons who refuse to be tested are subject to arrest. Wis. Stat. § 343.305

2. Forced Blood Draws: For many years Wisconsin allowed for warrantless, non-consensual blood draws, in Operating While Under the Influence (“OWI”) investigations. See State v. Bohling, 173 Wis.2d 529

   a) Bohling was wiped out by the United States Supreme Court in 2013 by Missouri v. McNeely, 133 S.Ct. 1552, where the high court rejected the notion that the dissipation of alcohol in the bloodstream is an automatic exigent circumstance. Accordingly McNeely requires search warrants in forced blood-draw cases.

   b) Wisconsin is the only state in the country that does not criminalize OWI first offense. This created a problem in meeting the McNeely requirement in those cases. The legislature responded by enacting 2015 Wisconsin Act 183, which allows for search warrants for the forfeiture/civil offense of OWI first offense.

D. Immunity for withdrawing blood. Wis. Stat. § 895.53 provides that any person—and any employer of the person—withdrawing blood at the request of a traffic officer, law enforcement officer or conservation warden for the purpose of determining the presence or quantity of alcohol, controlled substances, controlled substance analogs or any combination of alcohol, controlled substances and controlled substance analogs is immune from any civil or criminal liability for the act, except for civil liability for negligence in the performance of the act.

V. Practical tips for working together in a constructive manner

A. Be proactive: create an open dialogue with law enforcement to get on the same page.

B. Identify common ground.

   1. Public safety.

   2. Compliance with the law—including laws that protect a person’s privacy.

      a) Providers and law enforcement must both take privacy seriously
b) Law enforcement’s goal of solving crimes must be balanced with privacy law. Individuals don’t automatically lose privacy protections because a crime has been committed and is being investigated.

3. Recognize and be mindful of the different roles individuals play – to law enforcement, individuals are potential criminals or victims; to health care providers, those same individuals are patients or employees.

4. Consider developing a Memorandum of Understanding to outline responsibilities and mutual understandings.

C. Be consistent.

1. Have clear policies and procedures in place.
   a) Policies should be consistent with the mission and values of your organization.
   b) Procedures should make it clear who has authority to disclose PHI and when matters should be elevated.
   c) Identify staff members or departments who are most likely to come into contact with law enforcement, and make sure all of those staff members are appropriately trained and also capable of explaining privacy concerns to law enforcement. This will be your first line of creating an open dialogue with law enforcement.
   d) Provide resources to answer questions and provide advice to staff.
   e) Provide access only in accordance with the minimum necessary standard

This outline was prepared by Diane Welsh, Meghan O’Connor and David Perlman. It is not intended to serve as legal advice, or an alternative to obtaining appropriate legal counsel. The content does not necessarily reflect the views of the authors or their organizations.