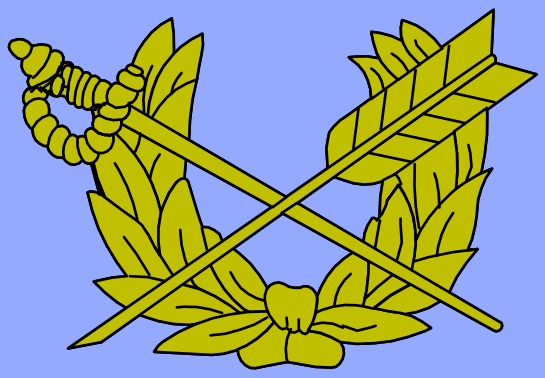
ADMINISTRATIVE AND CIVIL
LAW DEPARTMENT

GOVERNMENT INFORMATION PRACTICES (GIP) DESKBOOK 2022



The Judge Advocate General's School
United States Army

ADMINISTRATIVE AND CIVIL LAW DEPARTMENT

GOVERNMENT INFORMATION PRACTICES DESKBOOK

TABLE OF CONTENTS

*Chapter C is a compilation of HIPAA guidance from the U.S. Department of Health and Human Services, Defense Health Agency, and Military Health System.

August 2022

CHAPTER A

FREEDOM OF INFORMATION ACT

5 USC §552

Outline

I. REFERENCES.

A. Primary Sources.

1. Freedom of Information Act, 5 U.S.C. § 552, *as amended* [most recently by the "FOIA Improvement Act of 2016," signed 30 June 2016].

2. Title 32, Code of Federal Regulations, Part 286, DoD Freedom of Information Act (FOIA) Program (effective 5 January 2017).

3. Department of Defense Manual 5400.07, DoD Freedom of Information Act (FOIA) Program (25 January 2017).

4. Army Regulation No. 25-55, The Department of the Army Freedom of Information Act Program (19 October 2020).

5. Air Force Manual, DoDM 5400.07_AFMAN 33-302, Freedom of Information Act Program (27 April 2018).

6. Secretary of the Navy Instruction 5720.42G, Department of the Navy Freedom of Information Act Program (15 January 2019).

7. Commandant's Instruction M5260.3 - The Coast Guard Freedom of Information and Privacy Acts Manual (6 April 2005, Change 5).

B. Secondary Sources.

1. DoJ Guide to the Freedom of Information Act, a Department of Justice publication (available at https://www.justice.gov/oip/doj-guide-freedom-information-act-0) [hereinafter DoJ FOIA Guide]. Attorneys should refer to the DoJ FOIA Guide for current FOIA law and practices.

2. Freedom of Information Act Court Decisions Overview, a Department of Justice website containing summaries of FOIA court decisions (available at http://www.justice.gov/oip/court-decisions-overview). Attorneys can also subscribe to receive e-mail notifications on FOIA court decisions.

3. FOIA Update, a newsletter issued quarterly by the DoJ Office of Information Policy (OIP), from 1979-2000. Available on the DoJ FOIA web site at www.usdoj.gov/oip/foi-upd.htm.

4. FOIA Post, a web-based successor to DoJ's FOIA Update from 2001-2010, is available at https://www.justice.gov/oip/foia-post-1.

5. "Summaries of New Decisions" a feature of FOIA Post, a monthly compilation of all FOIA decisions received by the DoJ OIP from 2000-2010, is available at https://www.justice.gov/oip/foia-post-2000-2010.

6. Military Resources Available On-Line.

a. Department of Defense - http://open.defense.gov/Transparency/FOIA.aspx

b. Army – https://www.rmda.army.mil/foia/RMDA-FOIA-Division.html

c. Navy – http://foia.navy.mil

d. Marine Corps – http://www.hqmc.marines.mil/Agencies/USMCFOIA.aspx

e. Air Force – http://www.foia.af.mil/

f. Coast Guard – http://www.uscg.mil/foia

II. INTRODUCTION.

A. History/Purpose.

1. The Freedom of Information Act (FOIA) was enacted in 1966, and took effect 5 July 1967. It revised the public disclosure section of the Administrative Procedure Act. 5 U.S.C. § 1002 (1964) (enacted in 1946, amended in 1966, and now codified at 5 U.S.C. § 552).

2. "The basic purpose of the FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978). The FOIA firmly established an effective statutory right of public access to executive branch information in the federal government.

B. Key Concepts.

1. Applies to any and all agency records within the government's possession and control.

2. Disclosure is the rule, not the exception.

3. Generally, the status of the requester and purpose of a request are irrelevant with respect to what records are disclosed. [Requester status is relevant regarding expedited access, fees, and attorney fees].

4. The government has the burden to justify withholding of information.

5. The requester may seek administrative and judicial relief if access to government information is improperly denied.

III. RELEASING AGENCY RECORDS.

A. Publication. § 552(a)(1) (Requires disclosure of agency procedures, substantive rules, functions, organization and general policy through Federal Register publication).

1. How to obtain information from the agency: DoDM 5400.07, AR 25-55, DoDM 5400.07/AFMAN 33-302, SECNAVINST 5720.42G.

2. Rules of procedure and how to make submissions to the agency: Federal Acquisition Regulation (FAR), DoD FAR Supp., and Army FAR Supp. (AFARS)(contract submissions).

3. Substantive rules of general applicability. NI Industries v. United States, 841 F.2d 1104 (Fed. Cir. 1988); Vigil v. Andrus, 667 F.2d 931 (10th Cir. 1982); United States v. Mowat, 582 F.2d 1194 (9th Cir. 1978); Pruner v. Department of the Army, 755 F. Supp. 362 (D. Kan. 1991).

B. "Reading Room" Materials. § 552(a)(2) (Requires agency to make "available for public inspection and copying" records of final opinions, policy statements, administrative staff manuals, and frequently requested material.) Stanley v. Department of Defense, et al., No. 98-CV-4116 (S.D. Ill. June 22, 1999) (military hospital operational manuals are "internal housekeeping rules" as opposed to the kind of material of interest to the general public.)

1. Final opinions rendered in the adjudication of cases, specific policy statements, and certain administrative staff manuals. Vietnam Veterans of America v. Department of the Navy, 876 F.2d 164 (D.C. 1989).

2. The agency does not need to make available materials "related solely to the [agency's] internal personnel rules and practices." Hamlet v. United States, 63 F.3d 1097 (Fed. Cir. 1995), *see*, DoJ FOIA Guide.

3. Copies of disclosed records, frequently requested under FOIA (generally, three approved requests).

4. Reading Room records created after 1 November 1996 must be available on an agency's website.

5. Index for Public Inspection- final opinions of adjudicated cases; policies statements and interpretations not published in Federal Register; administrative staff manuals and instructions that affect a member of the public; frequently requested records that have been previously released.

C. Release Upon Request. § 552(a)(3). This is the most common means by which the public accesses Government records (and the subject of the remainder of this outline.)

IV. KEYS TO UNDERSTANDING THE FOIA.

A. Key Definitions.

1. What is an "agency?" § 552(f). "Agency" means "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency."

a. However, the Office of the President and those organizations within the Executive Office of the President whose function is limited to advising and assisting the President are excluded from the definition of agency.

b. Subdivisions of an agency are not treated as independent agencies. Judicial Watch, Inc. v. FBI, 190 F.Supp.2d 29, 30 n.1 (D.D.C. 2002) (stating that proper defendant is the Department of Justice "rather than the FBI, which is a component of DOJ and therefore not an "agency" within the statutory definition").

c. **The Department of Defense (DoD) is our agency**.

(1) The Departments of the Army, Air Force, and Navy are components of an agency. Schwartz v. General Accounting Office, No. 00-369, (D.D.C., Nov.13, 2001) (subdivisions of an agency and individual employees are not proper party defendants under the FOIA).

(2) Federally recognized Army National Guard units are considered part of the Army, therefore, they fall within the definition of an "agency" for FOIA and Privacy Act purposes. In Re: Sealed Case, 551 F.3d 1047 (D.C. Cir. 2009)(holding that as long as the Secretary of the Army has not withdrawn a National Guard's federal recognition, it is part of an agency for purposes of the Privacy Act [and thus the FOIA's] whether or not federally activated). The Privacy Act adopts the Freedom of Information Act's definition of agency (5 USC § 552a(a)(1)).

d. Under the FOIA, the term agency does not include:

(1) Congress, Judiciary, Office of the President (including Advisors), or state agencies. Wright v. Curry, 122 F.App'x 724, (5th Cir. 2004) (state agencies are "expressly exclude[d]" from scope of FOIA); Armstrong v. Executive Office of the President, 90 F.3d 553 (D.C. Cir. 1996) (offices within the Executive Office of the President whose functions are limited to advising and assisting the President do not fall within the definition of "agency"), cert. denied, 117 S.Ct. 1842 (1997); Dow Jones & Co., Inc. v. Department of Justice, 917 F.2d 571 (D.C. Cir. 1990) (Congress is not an agency for FOIA); Dong v. Smithsonian

Inst., 125 F.3d 877 (D.C. Cir. 1997) (holding that Smithsonian lacks both the "authority" necessary for it to qualify as an "authority of the government of the United States" under § 551(1) and the executive Department status necessary under § 552(f)), *cert. denied*, 524 U.S. 922 (1998)); Behar v. DHS, 2022 WL 2542015 (2d Cir. July 8, 2022) (holding that "[n]either a presidential campaign nor a transition qualifies as an 'agency' of the federal government under the FOIA. A transition receives government funding, but funding short of Government control leaves grantees free from the direct obligations imposed by the FOIA").

(2) Private organizations, unless the government engages in "extensive, detailed, and virtually day-to-day supervision." Burka v. HHS, 87 F.3d 508 (D.C.Cir. 1996) (finding data tapes created and possessed by contractor to be agency records because of extensive supervision exercised by agency which "evidenced" constructive control").

(3) Private citizens. *See* Allnut v. Department of Justice, 99 F.Supp. 2d 673 (D. Md. 2000) (records held by private trustee acting as agent for the federal government not subject to the FOIA).

2. What is a "record?" Information collected, produced or maintained by the government which is within the possession and control of the government and which is readily retrievable and reproducible.

a. "Readily Reproducible." Examples include: Books, papers, maps, and photographs, and machine readable materials, regardless of physical form. DoDM 5400.07, para. 3.12.

b. "Possession and Control." An agency must both possess and control the record. Department of Justice v. Tax Analysts, 492 U.S. 136 (1989) (agency must create or obtain the records and must have them in possession because of the legitimate conduct of agency business). DoDM 5400.07, para. 6.2.h.

(1) Possession of records created by another agency. McGehee v. CIA, 697 F.2d 1095 (D.C. Cir. 1983).

(2) Records generated from sources outside the Government. Records must be either government-owned or subject to substantial government control or use. Burka v. HHS, 87 F.3d 508 (D.C. Cir. 1996) (data tapes created and possessed by contractor are agency records because they are "constructively controlled" through agency's excessive supervision); Hercules, Inc. v. Marsh, 839 F.2d 1027 (4th Cir. 1988) (contractor-prepared Army post telephone directory is government record because book was government-financed and bore "Property of U.S." legend).

(3) Research Data. Amendment to the Fiscal Year 1999 Omnibus Appropriations Bill required modification of OMB Circular A-110 to allow private parties access to non-profit grantee-held research data through FOIA request [modifying Supreme Court decision in Forsham v. Harris, 445 U.S. 169 (1980) (which held records in possession of federal contractors not accessible under the FOIA even if records relate to contractor's contract with the agency)].

(4) Government contractors managing government records. OPEN Government Act of 2007 clarifies definition of "record" to include information "maintained for an agency by an entity under government contract, for the purpose of records management."

(5) Not agency records where records are not maintained under contract for records management. Historical records of calls maintained by Verizon Wireless, a government Blackberry service provider, do not qualify as "agency records" under 5 U.S. C. 552(f)(2)(B) because they are not "maintained for an agency by an entity under Government contract, for the *purposes of records management*." Amer. Small Bus. League v. SBA, 623 F.3d 1052 (9th Cir. 2010).

c. What is not a "record?"

(1) Personal records. Documents created or maintained without official requirement for the convenience of the creator as a memory refresher and not shared with others for agency use. *See* Bureau of Nat'l Affairs v. United States Department of Justice, 742 F.2d 1484 (D.C. Cir. 1984) (uncirculated appointment calendar and telephone message slips of agency official are not agency records); Fortson v. Harvey, 407 F.Supp. 2d 13 (D.D.C. 2005) (Army officer's notes of investigation were personal records because notes were used only to refresh officer's memory and were neither integrated into agency files nor relied on by other agency employees). DoDM 5400.07, para. G.2. "personal file." In determining whether a record is a "personal record," the D.C. Circuit has held that an agency should examine "the totality of the circumstances surrounding the creation, maintenance, and use" of the record. Factors relevant to this inquiry include, among others, (1) the purpose for which the document was created; (2) the degree of integration of the record into the agency's filing system; and (3) the extent to which the record's author or other employees used the record to conduct agency business. *See* Bureau of Nat'l Affairs v. United States Department of Justice, 742 F.2d 1484, 1492 (D.C. Cir. 1984).

(2) Tangible, evidentiary objects. Nichols v. United States, 325 F.Supp 130 (D. Kan. 1971) (archival exhibits consisting of guns, bullets, and clothing pertaining to assassination of President Kennedy are not records); Matthews v. United States Postal Service, No. 92-1208, slip op. at 4, n. 3 (W.D. Mo. Apr. 14, 1994) (computer hardware is not a record).

(3) Documents generated by and under the control of "non-agency" Federal entities. United States v. Anderson, Crim. No. 95-0040, 2003 U.S. LEXIS 725 (E.D. La. Jan. 16, 2003) (grand jury transcripts are court records and, therefore, are not agency records under the FOIA).

(4) A request for uncompiled data (selective information) is not a request for records. Borom v. Crawford, 651 F.2d 500 (7th Cir. 1981) (affirming summary judgment order denying request for parole data compiled by race when no such compilation existed); Krohn v. DOJ, 628 F.2d 195 (D.C. Cir. 1980).

d. The FOIA does not require agencies to create or retain records. Flight Safety Services Corp. v. Department of Labor, 326 F.3d 607 (5th Cir. 2003) (requester's demand that the agency "simply insert new information in the place of the redacted information requires the creation of new agency records, a task the FOIA does not require the government to perform"); DoDM 5400.07, para. 6.2.h.

(1) Agency does not have to respond to requester questions. Zemansky v. EPA, 767 F.2d 569 (9th Cir. 1985).

(2) DoD may create a new record when more useful to requester or less burdensome to agency. DoDM 5400.07, para 6.2.h.(1).

(3) While the FOIA does not require agencies to create or retain records, the Federal Records Act (now known as the National Archives Act), 44 U.S.C. § 2101 *et seq*., does require record retention pursuant to National Archives and Records Administration schedules. The National Archivist is presently involved in litigation over his orders regarding the retention/destruction of electronic mail/messages.

B. Key Factors Affecting Release.

1. Rule of Segregability. § 552(b); DoDM 5400.07, para. 5.1.e.

a. Must segregate and release portions of agency records not subject to a withholding exemption. Trans-Pacific Policing Agreement v. United States Customs Serv., 177 F.3d 1022 (D.C. Cir. 1999) (remanded for determination if 10- digit shipping code number could be segregated); Ogelsby v. Department of the Army, 79 F.3d 1172 (D.C. Cir. 1996); Army Times Publishing Co. v. Department of the Air Force, 998 F.2d 1067 (D.C. Cir. 1993).

b. Nonexempt material is not "reasonably segregable" when efforts to segregate amount to an inordinate burden on the agency. Lead Industries Association v. OSHA, 610 F.2d 70 (2d Cir. 1979).

2. Status and purpose of requester.

a. As a general rule, status and purpose of the requester are not considered

by the agency except in deciding procedural matters such as expedited processing and fee issues. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

b. A foreign government is a person under the Act. DoDM 5400.07, para. 6.1.b.(1); Neal-Cooper Grain Co. v. Kissinger, 385 F. Supp. 769 (D.D.C. 1974). **However, there are exceptions:**

c. The Intelligence Authorization Act of 2003, Public Law No. 107-306, 116 Stat. 2383 (2002) amended the FOIA, at 5 U.S.C. § 552(a)(3)(E)(ii), to preclude elements of the intelligence community from disclosing any records in response to a FOIA request made by any foreign government or international governmental organization, either directly or through a representative. Elements of the intelligence community are identified in 50 U.S.C. § 401a. (4) (Includes the Central Intelligence Agency; National Security Agency; Defense Intelligence Agency; and other elements within various Federal agencies).

d. Fugitives are not "persons" for purposes of the FOIA. Doyle v. Department of Justice, 668 F.2d 1365 (D.C. Dir. 1981) (fugitive is not entitled to enforcement of FOIA's access provisions because he cannot expect judicial aid in obtaining government records related to sentence that he was evading); *but see* O'Rourke v. Department of Justice, 684 F.Supp. 716 (D.D.C. 1988) (convicted criminal, fugitive from his home country and undergoing U.S. deportation proceedings, qualified as "any person" for FOIA purposes).

3. Previous releases.

a. "Release to one equals release to all."

b. Waiver issues. Students Against Genocide v. Department of State, 257 F.3d 828 (D.C. Cir. 2001) (exemptions were not waived when withheld photographs were displayed, but not distributed, by then-UN Ambassador Madeline Albright during presentation to U.N. Security Council).

4. The Reasonably Foreseeable Harm Standard.

a. The FOIA Improvement Act of 2016 requires agencies to apply a reasonably foreseeable harm standard when denying requests made after 30 June 2016.

b. Under the FOIA Improvement Act of 2016, an agency may deny release of records for requests under the FOIA only if:
(1) the agency reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions; or
(2) disclosure is prohibited by law.

5. Department of Defense Posture:

a. **Be deliberate and careful with all classified, controlled unclassified, and predecisional policy information and proposals.** [*See* Memorandum, Secretary of Defense, Subject: Reinforcing Operations Security and the Importance of Preventing Unauthorized Disclosures, dated 20 Jul 2010, at [https://media.defense.gov/2020/Jul/21/2002460476/-1/-1/1/REINFORCING_OPERATIONS_SECURITY_AND_THE_IMPORTANCE_OF_PREVENTING_UNAUTHORIZED_DISCLOSURES.PDF]

b. DoD is statutorily authorized to withhold personal identifying information related to personnel stationed overseas or with sensitive or routinely deploying units. [*See* 10 U.S.C. § 130(b).] Current policy requires a much greater protection of information post-9/11 and any information "that personally identifies DoD personnel [is to] be more carefully scrutinized and limited. Under this policy, personally identifying information may be inappropriate for inclusion in any medium available to the general public." [*See* Memorandum, Office of the Secretary of Defense, Subject: Withholding Information that Identifies DoD Personnel, dated 1 Sep 2005.]

6. Format of Records. The 1996 amendments to the Freedom of Information Act (the Electronic Freedom of Information Act Amendments, or "EFOIA") give the requester choice of format, where readily reproducible. Dayton Newspapers, Inc. v. Department of the Air Force, 35 F. Supp.2d 1033 (S.D. Ohio 1998); *but see* Students Against Genocide v. Department of State, 257 F.3d 828 (D.C. Cir. 2001) (agency is not required to produce new photographs at a different resolution in order to mask the capabilities of the reconnaissance systems that produced them; such a step is not merely a matter of requester's choice of "format").

V. PROCESSING REQUESTS FOR RELEASE.

A. Requirement for a Proper Request. DoDM 5400.07, paras. G.2."FOIA request."; 6.1.

1. Must request an "agency record." DoDM 5400.07, paras., G.2."agency record."; 6.3.b.(7).

2. Must reasonably describe the record. DoDM 5400.07. paras., G.2. "FOIA request."; 6.3.b.(5). *See* Ruotolo v. Department of Justice, 53 F.3d 4 (2d Cir. 1995); AFGE v. Department of Commerce, 907 F.2d 203 (D.C. Cir. 1990); Mason v. Calloway, 554 F.2d 129 (4th Cir. 1977).

3. Must conduct an initial determination. DoDM 5400.07, para. 6.3.

B. Required Agency Response. **Note:** Each service has established release and processing procedures. DoDM 5400.07, para. 6.1; AR 25-55, ch. V; DoDM 5400.07/AFMAN 33-302, Appendix 2; SECNAVINST 5720.42G, encls.(2)-(5).

1. Agency must advise requester of agency's receipt of the request and, if necessary, forward request to the proper agency records custodian.

2. Agency should liberally construe FOIA requests. *See* LaCedra v. Exec. Office for U.S. Attorneys, 317 F.3rd 345 (D.C. Cir. 2003) (in view of obligation "to construe a FOIA request liberally," reading of plaintiff's FOIA request -- for "all documents pertaining to my case . . . [and] specifically" for rewards and fingerprints -- to include only those specific items was "simply implausible" and "also wrong").

3. Agency must evaluate the request for processing priority. The Electronic FOIA amendments modified the court-sanctioned rule of "first-in, first-out" FOIA processing. Open America v. Watergate Special Prosecution Force, 547 F.2d 606 (D.C. Cir. 1976).

a. Agencies may establish "multi-track" processing in which requests are sorted in accordance with the complexity of the request or potential volume of responsive document.

b. Agencies must have procedures to for expedited processing when exceptional circumstances surround a request, such as an imminent threat to life or personal safety or if the requester is a "person primarily engaged in disseminating information" and there is an "urgency to inform the public of actual or alleged Federal Government activity." Al-Fayed v CIA, 254 F.3d 300 (D.C. Cir. 2001) (no expedited processing because there is no evidence that events connected to the deaths of Princess Diana and Dodi Al-Fayed are matters of "current exigency" to the American public); Tripp v. DoD, 193 F. Supp. 2d 229 (D.D.C. 2002) (expedited processing denied because requester is not "primarily engaged in the activity of disseminating information," even though "she has been the object of media attention, and has at times provided information to the media"; requester's "job application to the Marshall Center and the resulting alleged Privacy Act violations by DoD are not the subject of any breaking news story.").

c. Agency must make "reasonable efforts" to locate records and court may require agency to demonstrate adequacy of search. Dayton Newspapers, Inc. v. VA, 257 F.Supp. 2d 988 (S.D. Ohio 2003) (pursuant to its FOIA regulations, the VA was obligated to search only its headquarters, absent a clear indication that plaintiff sought records maintained in a VA regional office), *sustaining defendant's motion for summary judgment and ordering final judgment*, 510 F.Supp. 2d 441 (S.D. Ohio 2007); Blackman v. Department of Justice, No. 00-3004 (D.D.C. Oct. 9, 2001) (agency's search for deposition transcripts of one expert witness using "pay records" index was adequate; manual search that would involve 3,000 aviation cases and as many as 37 million pages would be "overly burdensome"), *summary affirmance denied*, No. 01- 5431 (D.C. Cir. Mar. 29, 2002) (*per curiam*)); Dayton Newspapers, Inc. v. Department of the Air Force, 35 F.Supp. 2d 1033 (S.D. Ohio 1998) (holding that 51 hours of electronic searching and assembly is "small price to pay").

4. Agency must **segregate and release** nonexempt information. Trans-Pacific Policing Agreement v. United States Customs Serv., 177 F.3d 1022 (D.C. Cir. 1999) (remanded for determination if 10 digit shipping code number could be segregated); Dynalectron Corp. v. Department of the Air Force, 1984 WL 3289 (D.D.C. Oct. 30, 1984). In accordance with the OPEN Government Act of 2007, the requester must be informed of the amount of redacted exempt material withheld and the specific exemption relied upon to withhold the information. *See also* DoDM 5400.07, para. 5.1.e.

5. IAW the 1996 EFOIA amendments, the agency must provide responsive records to the requester in the requester's selected format, when possible and reasonable. Dayton Newspapers, Inc. v. Department of the Air Force, 35 F. Supp.2d 1033 (S.D. Ohio 1998).

6. Proper agency officials must act upon the request. Records custodians cannot deny a request; only Initial Denial Authority (IDA) may deny requested records. *See* Enviro Tech Int'l, Inc. v. EPA, 2003 U.S. LEXIS 25493 (N.D. Ill. Mar. 11, 2003) (EPA failed to comply with its regulations when a staff person, rather than a division director, signed EPA's denial of plaintiff's FOIA request) *aff'd* 371 F.3d 370 (7th Cir. 2004).

7. Agency must document any reasons for not releasing a record. DoDM 5400.07, para. 6.3.b. The reasons may include:

a. No responsive records after a "reasonable" search. Gaines v. EEOC, 36 F.App'x 640 (9th Cir. 2002) ("no records" response appropriate where agency had no responsive records).

b. Agency neither controls nor otherwise possesses record.

c. Record no reasonably described.

d. Failure to comply with agency's procedural requirements.

e. Request is withdrawn.

f. Fee dispute.

g. Duplicate Request.

h. The information is not, by definition, a "record." Oglesby v. U.S. Department of the Army, 920 F.2d 57 (D.C. Cir. 1990).

C. Requirement to Meet Statutory Time Limits. 5 U.S.C. §§ 552(a)(6)(A) & (B).

1. Initial agency response - 20 working days.

a. Agencies have 20 days (excepting Saturdays, Sundays, and legal

public holidays) after receipt of a request to comply with or deny the request.

b. In "unusual circumstances," (i.e., voluminous amount of records, consultation with another agency, or retrieval of records from archival storage,) an agency may have an additional ten (10) day extension if the agency tells the requester in writing why it needs the extension and when it will make a determination on the request.

c. Agency's 20 day period to respond to a request commences on the date on which the request is first received by the "appropriate component of the agency, but in any event not later than ten days after the request is received by any component of the agency" designated by the agency to receive requests**.**

d. Agency is allowed to make one request to the requester for information and toll the 20-day period while it awaits the information. Also, agency may toll the 20- day period as often as necessary to clarify with the requester an issue regarding fees. Either tolling period ends upon receipt of the information or clarification sought.

e. Requester dissatisfied with adverse agency response - shall be advised of the right to file an appeal with the agency appellate authority no later than **90 calendar days** from the date of receipt of the agency response, and the right to seek dispute resolution services. DoDM 5400.07, para. 6.5; 32 CFR § 286.11.

f. Failure to process timely; fee waiver; ruling that where agency did not act on request by plaintiff (an "all other requester" category requester) for fee waiver, nor act on his administrative appeal, within 20 working days, it could not charge search fees; when requester responded to agency's letter seeking more information concerning the fee waiver, that stopped the tolling of the 20-day period. Bensman v. Nat'l Park Serv., No. 10-1910, 2011 WL 3489507 (D.D.C. Aug. 10, 2011).

g. If agency shows failure to meet time limits was result of "exceptional circumstances" and it is applying due diligence in processing request, then court can allow additional time for administrative processing of request. §552(a)(6)(C). Open America v. Watergate Special Prosecution Force, 547 F.2d 605 (D.C. Cir. 1976).

h. "Exceptional circumstances" does not include delays that result from a predictable agency workload of requests unless "the agency demonstrates reasonable progress in reducing its backlog of pending requests." 5 U.S.C. § 552(a)(6)(C)(ii).

2. Agency response to Appeals - 20 working days.

3. Denial and "constructive denial" of requests.

a. Custodian cannot deny a request. *See* Enviro Tech Int'l, Inc. v. EPA, No. 02 C4650 (N.D. Ill. Mar. 11, 2003) (EPA failed to comply with its regulations when a staff person, rather than a division director, signed EPA's denial of plaintiff's FOIA request).

b. Records withheld by custodians must be forwarded to the Initial Denial Authority (IDA) for decision on denials.

c. An agency's failure to comply with the time limits for either the initial request or the administrative appeal may be treated as a "constructive exhaustion" of administrative remedies, and a requester may immediately seek judicial review. § 552(a)(6). *See*, Spannaus v. United States Department of Justice, 824 F. 2d 52 (D.C. Cir. 1987).

D. Documenting Agency Action on Requests.

1. Congress requires an annual FOIA processing report to be compiled by each agency. 5 U.S.C. § 552(e)(1). The FOIA Improvement Act of 2016 added additional requirements that must be reported. Generally, reporting requirements include: the number of requests for records pending at end of the fiscal year; the average and median number of days that such requests had been pending; the number of requests for records received by the agency; the number of requests that the agency processed; the average and median number of days taken by the agency to process different types of requests; the number of determinations made by the agency not to comply with requests for records made to the agency, and the reasons for each such determination, etc.

2. DoD components capture data related to FOIA processing on DD Form 2086, Record of Freedom of Information (FOI) Processing Cost. In 2008, the Army implemented the Freedom of Information and Privacy Acts Case Tracking System (FACTS). FACTS is a web-based program designed to provide uniform data collection, reporting, and tracking of Army FOIA requests. Its use is **mandatory** by Army organizations.

3. Each agency is required to make its annual report available on its web site and the Department of Justice is required to link all such reports at one site.

E. Calculating Fees & Processing Fee Waiver Requests.

1. Agencies can require requesters to defray certain costs of agency response.

a. The 1966 FOIA permitted agencies to charge fees for services.

b. The 1974 amendments permitted collection of fees for direct expenses only (i.e., duplication and search).

c. In 1986, Congress distinguished between various classes of requesters and established separate fee categories.

d. The OPEN Government Act of 2007 prohibits agencies from collecting search and duplication fees if the agency fails to comply with any time limit,

unless an unusual or exceptional circumstance applies to the processing of the request.

2. FOIA Processing Fees. Charges are based on requester's status and purpose. There are three categories of requesters:

a. First - Most favored category: (1) educational, (2) noncommercial scientific institutions (whose purpose is scholarly or scientific research), and (2) representatives of the news media are charged only for duplication costs after the first 100 pages. *See* Elec. Privacy Info. Ctr. v. DoD, 241 F.Supp. 2d 5 (D.D.C. 2003) (plaintiff, a nonprofit, tax-exempt, educational organization, is a "representative of the news media" for purposes of the FOIA; the determinative question is the organization's "activities," not its corporate structure; plaintiff publishes a biweekly electronic newsletter and has compiled and published 7 books relating to privacy and civil rights; merely maintaining a Web site, by itself, is insufficient to qualify a FOIA requester as a representative of the news media); National Security Archive v. Department of Defense, 880 F.2d 1381 (D.C. Cir. 1989); Stanley v. Department of Defense, et al. No. 98-CV-4117 (S.D. Ill. June 22, 1999).

b. Second - Least favored category: requesters of records for commercial use are charged for search, duplication, and review.

c. Third category: All other requesters are charged for search after the first 2 hours and duplication after the first 100 pages.

3. DoD FOIA Hourly Processing Fee Rates. Effective 5 January 2017. 32 CFR § 286.

a. DoD Search and review costs.

(1) Administrative (E1–E9/GS1–GS8): $24.00 per hour.

(2) Professional (O1–O6/W1–W5/GS9–GS15): $48.00 per hour.

(3) Executive (O7 and above and Senior Executive Service): $110.00 per hour.

(4) Contractor: $48.00 per hour.

b. Duplication costs. Flat rate for office copy reproduction is $.15 per page.

4. Fee restrictions.

a. Under the FOIA Improvement Act of 2016, agencies shall not assess search fees against commercial or "other" requesters, or duplication fees against representatives of the news media or educational requesters, if the agency does not respond within 20 working days.

(1) When it is determined that unusual circumstances (documents not located with the office processing the FOIA request, the responsive records are voluminous, and consultation with another agency) apply, the agency is granted another 10 days before this fee restriction applies. However, the agency must provide timely written notice to the requester of the unusual circumstances.

(2) This fee restriction does not apply if the responsive records total more than 5,000 pages and the DoD Component has provided a timely written notice to the requester and made three or more good faith attempts to discuss, with the requester, how to effectively limit the scope of the request.

b. No fee will be charged when the total fee, after deducting the 100 free pages (or its cost equivalent) and the first two hours of search, is equal to or less than $25. 32 CFR § 286.12(e)(5).

c. When the agency estimates or determines that allowable charges are likely to exceed $250.00, notify the requester and obtain satisfactory assurance of full payment, or for advance payment of up to full amount in the case of requester with no history of payment. 32 CFR § 286.12(j).

d. Where a requester has previously failed to pay a properly charged FOIA fee to any agency within 30 calendar days of the billing date, a DoD Component may require that the requester pay the full amount due, plus any applicable interest on that prior request, and the DoD Component may require that the requester make an advance payment of the full amount of any anticipated fee before the DoD Component begins to process a new request or continues to process a pending request or any pending appeal. 32 CFR § 286.12(j)(3).

5. Requests for Fee Waiver. Unlike the substantive FOIA analysis, waivers may be based on the requester's status and motive. *See* Schulz v. Hughes, 250 F.Supp. 2d 470 (E.D. Pa. 2003) (plaintiff not entitled to a waiver of fees; the release of information concerning plaintiff's prosecution would not make a significant contribution to the public understanding of federal prosecutions or incarceration); McClellan Ecological Seepage Situation v. Carlucci, 835 F.2d 1282 (9th Cir. 1987) (applying and implicitly approving DoD's regulatory implementation of fee waiver provision).

F. Litigating Denied and Constructively Denied FOIA Requests.

1. Requester must exhaust administrative remedies. 5 U.S.C. § 552(a)(6)(C)(i).

a. Once an agency has responded to a request, regardless of whether the response is timely, the requester can seek judicial review only after appealing to the agency first. *See* Ford v. U.S. Department of Justice, No. 02-7538 (4th Cir. Feb. 5, 2003) (*per curiam*) (affirms district court ruling that plaintiff has not exhausted his administrative remedies where the FBI did not timely respond to his FOIA request but responded before suit was filed, and

where the agency denied as untimely plaintiff's appeal of the initial denial because he sent it nearly 10 years after the adverse decision); Hogan v. Huff, 2002 U.S. Dist. LEXIS 11092 (S.D.N.Y. June 21, 2002) (plaintiff failed to take legal action before the arrival of the first set of responsive records); Judicial Watch v. F.B.I., 190 F.Supp. 2d 29 (D.D.C. 2002).

b. A requester's failure to pay FOIA fees constitutes a failure to exhaust administrative remedies. *See*, Oglesby v. Department of the Army, 920 F.2d 57, 66 (D.C. Cir. 1990) (exhaustion does not occur until the required fees are paid or an appeal is taken from the refusal to waive fees).

c. Case is not ripe for adjudication when withholding of records was based upon requester's failure to pay fees associated with a FOIA request. Pietrangelo v. U.S. Department of the Army, 155 F.App'x 526 (2d Cir. 2005) (affirming dismissal for failure to exhaust, despite agency's untimely response, because plaintiff neither paid nor requested waiver of assessed fees).

2. The circumstances which would authorize a judicial stay were narrowed by E-FOIA amendments. Open America v. Watergate Special Prosecution Force, 547 F.2d 605 (D.C. Cir. 1976). Stays are granted for delays resulting from predictable agency workload of requests only if the agency "demonstrates reasonable progress in reducing its backlog of pending requests."

3. Judicial Review. 5 U.S.C. § 552(a)(4)(B).

a. Civil action challenging the denial of a request may only be brought by the person who filed the FOIA request. Three Forks Ranch Corp. v. Bureau of Land Mgmt, 358 F.Supp. 2d 1 (D.D.C. 2005) (holding that "a FOIA request made by an attorney must clearly indicate that it is being made 'on behalf of' the corporation to give that corporation standing to bring a FOIA challenge.").

b. Agency, not agency employee, is the proper party defendant. Petrus v. Bowen, 833 F.2d 581 (5th Cir. 1987) ("Neither the Freedom of Information Act nor the Privacy Act creates a cause of action against an individual employee of the agency.").

c. Scope of review - *de novo*.

d. *In camera* inspection is "within the broad discretion of the court." Quinon v. FBI, 86 F.3d 1222 (D.C. Cir. 1996).

e. Discovery is not typically part of a FOIA lawsuit. Heily v. U.S. Department of Commerce, 69 F.App'x 171 (4th Cir. 2003) ("It is well-established that discovery may be greatly restricted in FOIA cases.")

(1) The decision to permit discovery in FOIA cases rests with the district court judge. Wood v. FBI, 432 F.3d 78 (2d Cir. 2005).

(2) When discovery is permitted it is to be sparingly granted. Most

often, discovery is limited to investigating the scope of the agency search for responsive documents, the agency's indexing procedures, and similar issues. Schiller v. INS, 205 F. Supp. 2d 648 (W.D. Tex. 2002).

(3) Note: Though not designed to be a federal "discovery tool," the FOIA is frequently used as such by litigants in non-FOIA cases. *See* Pa. Department ofPub. Welfare v. United States, 2006 U.S. Dist. LEXIS 92807 (W.D. Pa. Dec. 21, 2006) (rejecting agency's argument that simply because the requester has another non-FOIA lawsuit against the agency, its FOIA request is "abusing or misusing FOIA to obtain non-discoverable documents").

(a) Discovery, particularly when a protective order is granted, generally provides greater access to all relevant records or records that could lead to relevant evidence than that provided by the FOIA.

(b) The FOIA is not a substitute for discovery in criminal cases. *See* Boyd v. DEA, 2002 U.S. Dist. LEXIS 27853 (D.D.C. Mar 8, 2002).

f. Vaughn index. A court may order an agency to submit a detailed index of the documents it seeks to withhold and the reasons justifying such withholding. Vaughn v. Rosen, 484 F.2d 820 (D.C. Cir. 1973); *Compare*, Wiener v. FBI, 943 F.2d 972 (9th Cir. 1991) *with* Maynard v. CIA, 986 F.2d 547 (1st Cir. 1993).

(1) The Vaughn index requires a correlation of the information that an agency decides to withhold with the particular FOIA exemption and the agency's justification for withholding. The index includes a general description of each document sought by the FOIA requester and explains the agency's justification for nondisclosure of each individual document or portion of a document.

(2) The index compels the agency to scrutinize any material withheld in justification of its claimed exemption, assists the court in performing its duties, and gives the requester as much information as is legally permissible.

g. Burden of proof. Burden is on the government to establish that a document is exempt from disclosure. 5 U.S.C. § 552(a)(4)(B).

4. Attorney Fees and Costs. § 552(a)(4)(E).

a. Attorney fees are within the discretion of the court when a FOIA plaintiff "substantially prevails." State of Texas v. Interstate Commerce Commission, 935 F.2d 728 (5th Cir. 1991); Education/Instruction, Inc. v. HUD, 649 F.2d 4 (1st Cir. 1981).

(1) Before 2002, the courts determined whether a plaintiff "substantially prevailed" by determining whether prosecution of the action was needed

and that action had a causative effect on delivery of information (i.e., the "catalyst theory"). Weisberg v. Department of Justice, 848 F.2d 1265 (D.C. Cir. 1988).

(2) After 2002, the courts required that "in order for plaintiffs in FOIA to become eligible for an award of attorney's fees, they must have been awarded some relief either in a judgment on the merits or in a court-ordered consent decree." Oil, Chemical & Atomic Workers Int'l Union v. Department of Energy, 288 F.3d 452 (D.C. Cir. 2002).

(3) However, "substantially prevailed" is defined as the obtaining of relief through a judicial order, or an enforceable written agreement, or by a voluntary or unilateral change in position by the agency, if the complainant's claim is not insubstantial. This is a return to the "catalyst theory" of substantially prevailed as described in Weisberg.

(4) All fees assessed in FOIA litigation must be paid by the agency from its annual appropriations. *See* DoD 7000.14-R, Financial Management Regulation, Volume 10, Chapter 12, Section 120201 ("It is Department funding policy that the attorneys' fees and other costs assessed in the FOIA litigation are to be paid from operating funds of the Military Department, Defense Agency, Field Activity or Combatant Command responsible for administering the initial FOIA determinations or contested record searches that are the subject of the litigation.").

b. No attorney fees for *pro se* litigants, Burka v. HHS, 87 F.3d 508 (D.C. Cir. 1996), although a law firm representing itself is eligible to claim attorney fees. Baker & Hostetler LLP v. U.S. Department of Commerce, 473 F.3d 312 (D.C.Civ. 2006).

c. Four factors that courts will generally consider to determine whether an award of fees and costs is appropriate under FOIA after determining the requester's eligibility:

(1) Benefit to the public derived from the case;

(2) Commercial benefit to the requester;

(3) Nature of requester's interest in the records sought; and

(4) Whether the agency's withholding of records had a reasonable basis in law. *See* Church of Scientology v. USPS, 700 F.2d 486 (9th Cir. 1983); LaSalle Extension University v. FTC, 627 F.2d 481 (D.C. Cir. 1980).

d. Commercial requesters and those requesters seeking information for commercial gain should be allowed attorney fees only where there is clear and positive benefit to the public and where the agency withheld information without a reasonable basis in law. Tax Analyst v. U.S. Department of Justice,

965 F.2d 1092 (D.C. Cir. 1992); c*f.* Aviation Data Service v. FAA, 687 F.2d 1319 (10th Cir. 1982).

5. Six year statute of limitations for filing FOIA lawsuits. 28 U.S.C. § 2401; Spannus v. DOJ, 824 F.2d 52 (D.C. Cir. 1987).

VI. NINE EXEMPTIONS PERMIT WITHHOLDING.

A. **Exemption 1: Classified Records**. This exemption protects matters that are "(A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive Order."

1. Threshold: To qualify for withholding under Exemption 1, a record must be substantively and procedurally properly classified.

2. Classifications are governed by Executive Order. On 29 December 2009, President Obama signed Executive Order 13526 which outlines how classified information should be handled. This order revokes and replaces the previous Executive Orders in effect, which were EO 12958 and EO 13292. The EO is implemented by DoDM 5200.01-Vol. 1.

a. There are three security classifications: Confidential, Secret, Top Secret. Classification is based upon the potential harm which could result from improper release of the protected documents, information, or materials.

b. For Official Use Only (FOUO). For FOUO information, see Glossary to DoDM 5200.01-Vol. 1. While not a proper classification under EO 13526, FOUO information may qualify for withholding under another FOIA exemption.

c. "Controlled Unclassified Information" is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 13526, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. President's Memorandum to the Heads of Executive Departments and Agencies, subject: Designation and Sharing of Controlled Unclassified Information (CUI), 44 WEEKLY COMP. PRES. DOC. 673 (May 7, 2008). This categorical designation, with accompanying document markings, is currently being implemented Government-wide and will replace markings currently used for sensitive but unclassified information within DoD (e.g., FOUO, FOUO- LES, LIMITED DISTRIBUTION). Memorandum from David M. Wennegren, DoD Deputy Chief Info. Officer, to Secretaries of the Military Departments, subject: Transition to New Markings for Controlled

Unclassified Information (CUI) (Dec. 28, 2007).

3. Segregability applies even in Exemption 1 cases. Ogelsby v. Department of the Army, 79 F.3d 1172 (D.C. Cir. 1996); Oglesby v. Department of the Army, 920 F.2d 57 (D.C. Cir. 1990). [In 1974, following the Court's decision in EPA v. Mink, 410 U.S. 73 (1973), Congress amended the FOIA to require the segregation of nonexempt material in Exemption 1 cases and to permit *in camera* inspections.]

4. Proper classification of records does not obviate the introduction of classified information in litigation.

a. Court conducts *de novo* review of both procedural and substantive propriety of classification. Allen v. CIA, 636 F.2d 1287 (D.C. Cir. 1980).

b. Court may conduct *in camera* inspection, although the court should give substantial weight to agency affidavits. Young v. CIA, 972 F.2d 536 (4th Cir. 1993).

c. Courts will give great deference to agency's expertise and judgment on classification. James Madison Project v. National Archives and Records Administration, 2002 U.S. App. LEXIS 11184 (D.D.C. Mar 5, 2002) (deferring to CIA decision to retain classification of 80-year old records relating to invisible inks), aff'd 2002 U.S. App. LEXIS 21427 (D.C. Cir. Oct. 11, 2002); Weatherhead v. United States, 157 F.3d 735 (9th Cir. 1998), *cert. granted*, 120 S. Ct. 34 (1999), *cert. dismissed and vacated*, 120 S.Ct. 577 (1999) (Court dismisses for mootness, but vacates 9th Circuit's holding that classification decisions are not given deference unless agency first makes acceptable showing of harm); Goldberg v. Department of State, 818 F.2d 71 (D.C. Cir. 1987); Taylor v. Department of the Army, 684 F.2d 99 (D.C. Cir. 1982). *See also* Ctr. for Nat'l Sec. Studies v. United States Department of Justice, 331 F.3d 918 (D.C. Cir. 2003) (in this post 9/11 case, court declares that it could not "conceive of any reason to limit deference to the executive in its area of expertise to certain FOIA exemptions [i.e., Exemptions 1 and 3] so long as the government's declarations raise legitimate concerns that disclosure would impair national security."); Am. Civil Liberties Union v. Department of Justice, No. 02-2077, 2003 U.S. Dist. LEXIS 8363 (D.D.C. May 19, 2003) (disclosure of statistical information regarding the Justice Department's use of surveillance and investigatory tools authorized by the USA PATRIOT Act would reveal intelligence activities, sources, or methods and could be expected to damage national security).

5. Operational Security.

a. Post-request classification is authorized. EO 13526, section 1.7(d), DoDM 5400.07, para. 5.2.a.

b. Compilation/Mosaic Theories of classification. The government may withhold apparently harmless bits and pieces of seemingly innocuous information, which when assembled together would reveal classified or exempt information. American Friends Serv. Comm. V. Department of Defense, 831 F.2d 441 (3d Cir. 1987); Taylor v. Department of the Army, 684 F.2d 99 (D.C. Cir. 1982); Halperin v. CIA, 629 F.2d 144, 150 (D.C. Cir. 1980). Use of the mosaic theory is not limited to Exemption 1 situations.

c. Previous Release of Classified Records Does Not Prevent Subsequent Withholding of Similar Type of Information. Aftergood v. CIA, 1999 U.S. Dist. LEXIS 18135 (D.D.C. Nov. 15, 1999) (CIA properly withheld its fiscal year 1999 total budget request because it may damage national security and reveal "intelligence sources and methods" even though it released the previous two years' budgets).

d. In rare cases mere existence of particular records may be classified. Phillippi v. CIA, 546 F.2d 1009 (D.C. Cir. 1976) (request for procurement records concerning Glomar Explorer submarine-retrieval ship; consequently "neither confirm nor deny" response known as "Glomar" response or "Glomarization").

(1) Glomar Denials or Glomarization is the agency's refusal to confirm or deny the existence or nonexistence of requested information or an abstract fact in cases where the sensitive fact or sensitive information would be disclosed by any other response to a particular FOIA request. *See* Kelly v. CIA, No. 00-2498 (D.D.C. Aug. 8, 2002) (CIA properly refused to confirm or deny the existence of any records reflecting a covert relationship between the CIA and UCLA because disclosure of whether such records (and activity) exist in relation to any particular academic institution would reveal intelligence sources and methods and would damage national security; exemption protection is not waived by 2 agency memoranda that are general discussions of the CIA's overt and covert relationships with academic institutions in general that have nothing to do with the any specific relationship with UCLA).

(2) Use of Glomar denial not limited to Exemption 1 cases. *See* DoDM 5400.07, para. 5.1.f.(1); FOIA Update Vol.VII, No. 1 (1986).

B. **Exemption 2: Internal Personnel Rules and Practices**. This exemption authorizes withholding an agency's internal rules and regulations governing matters pertaining to personnel or human resources.

1. Threshold: The record must be related "solely to internal personnel rules and practices of an agency."

2. Until March of 2011, Exemption 2 was generally interpreted by courts to

include two different bases for withholding records from release. These differing bases for withholding were commonly known as “Low 2” and “High 2.” The Supreme Court decision in *Milner v. Dep’t of the Navy*, 131 S. Ct. 1259 (March 7, 2011) The opinion essentially did away with “High 2” by narrowing the exemption to the “Low 2” version of the exemption.

a. The Court found the common understanding of the term “personnel rules and practices” when applied by other courts has resulted in little difficulty in determining what qualifies as one of those records. These records “share a critical feature: They concern the conditions of employment in federal agencies—such matters as hiring and firing, work rules and discipline, compensation and benefits.” *Id.* at 1265. The court declared that its “construction of the statutory language simply makes clear that Low 2 is all of 2 (and that High 2 is not 2 at all…).” *Id.*

b. “Exemption 2, consistent with the plain meaning of the term 'personnel rules and practices,' encompasses only records pertaining to issues of employee relations and human resources.” *Milner*, at 1271.

c. A New Three-Part Test: (1) The information must be related to “Personnel” Rules and Practices; *Id.* at 1265 (2) the information must “solely” relate to those personnel rules and policies; and (3) the information must be “internal” to the agency for their records and use. *See id.* at *1265 n.4*.

3. Because of the of the *Milner* decision, it may be helpful to understand the distinction that used to be drawn between “Low 2” and “High 2.”

a. The Court of Appeals for the District Court of Columbia Circuit was the leading case interpreting Exemption 2. In *Crooker v. ATF,* 670 F.2d 1051 (1981) the court interpreted the statutory language to create a two-part test for determining the meaning and application of Exemption 2. For records to qualify, first they had to be “predominantly internal,” and secondly they had to be of no genuine public interest (Low 2) or of a nature that would risk circumvention of the law (High 2). *See id.* at 1073-74.

b.“Low 2” applied to trivial matters and information in which there is little or no public interest. Even this interpretation of the exemption has been narrowed by *Milner* to clarify that it applies only to internal personnel rules and practices.

c. “High 2” provided authority to withhold information which would provide a requester with the means to circumvent an agency regulation or frustrate an agency function or mission. Examples of withholding under High 2: information concerning the design, array, structure, and construction of ammunition storage facilities; unclassified rules of engagement even though the enemy may be aware of the ROE through experiences with U.S. forces in Iraq; blueprint of agency buildings where contents or infrastructure could be harmed by public disclosure.

C. **Exemption 3: Other Federal Withholding Statutes**. FOIA Exemption 3 permits withholding of information prohibited from disclosure by another statute. A listing of Exemption 3 statutes claimed by agency (each fiscal year is available at: http://www.foia.gov.

1. Threshold: One of two disjunctive requirements must be met to withhold under this exemption: the withholding statute must either "(A) [require] that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establish particular criteria for withholding or refer to particular types of matters to be withheld." A statute falls within the exemption's coverage if it satisfies either one of its disjunctive requirements.

2. Examples of federal withholding statutes:

a. The Homeland Security Act of 2002, Public Law 107-296, includes a provision that operates as an Exemption 3 statute for "critical infrastructure" information that is obtained by DHS.

b. 42 U.S.C. § 290dd-3, Confidentiality of patient records in an alcohol and drug treatment program.

c. 10 U.S.C. § 1102, DoD Medical Quality Assurance Records.

d. 10 U.S.C. § 2305 and 41 U.S.C. § 253b, prohibiting release of certain contractual proposals.

e. 10 U.S.C. §130b, allows withholding of information on personnel of overseas, sensitive, or routinely deployable units. See Windel v. United States, 2005 U.S. Dist. LEXIS 44422 (D. Alaska Apr. 11, 2005), (applying protection to members of a routinely deployable unit of the Air National Guard). Pursuant to DoD guidance issued on 9 November 2001, all DoD components shall ordinarily withhold *lists* of names and other personally identifying information of currently or recently assigned personnel (citing privacy and security concerns). Names, other than lists, mentioned in other documents may be withheld if the release would raise substantial security or privacy concerns (utilize Exemption 6).

f. 10 U.S.C. §130e, allows withholding of information that is determined to be Department of Defense critical infrastructure security information and the public interest consideration in the disclosure does not outweigh preventing the disclosure of the information. Department of Defense critical infrastructure security information means sensitive but unclassified information that, if disclosed, would reveal vulnerabilities, result in significant disruption, destruction or damage of or to DoD operations, property or facilities. These facilities are those owned by or operated on behalf of the DoD. [This responds directly to the issues in *Milner*.]

g. See annual DoD FOIA Report for complete listing of Exemption 3 statutes relied upon by DoD during the reporting period.

3. Statutes **commonly mistaken** for Exemption 3 withholding statutes:

a. 18 U.S.C. § 1905; The Trade Secrets Act does not qualify because it prohibits only those disclosures "not authorized by law." CNA Fin. Corp. v. Donovan, 830 F.2d 1132 (D.C. Cir. 1987).

b. 5 U.S.C. § 552a; The Privacy Act.

c. 41 U.S.C. § 423(a)(1); The Procurement Integrity Act does not qualify because it prohibits only those disclosures "other than as provided by law" and "does not . . . limit the applicability of any . . . remedies established under any other law or regulation." *Cf*. Pikes Peak Family Housing, LLC v. United States, 40 Fed.Cl. 673 (1998) (provision does not prohibit disclosure in civil discovery because that is "provided by law"). *But see* Legal & Safety Employer Research, Inc. v. Department of the Army, 2001 U.S. Dist. LEXIS 26278 (E.D. Cal. May 7, 2001) (erroneously holding that the provision qualifies as an Exemption 3 statute).

4. Statutes may have retroactive application. *See* Sw. Ctr. for Biological Diversity v. USDA., 314 F.3d 1060 (9th Cir. 2002) (the court properly applied a recently enacted Exemption 3 statute in existence at the time of its decision [16 U.S.C. § 5937], rather than the law that was in existence at the time the suit was filed; statute protects information identifying the location of northern goshawk nest sites).

5. Carefully worded appropriations acts may qualify under Exemption 3. *See* City of Chicago v. U.S. Department of Treasury, 423 F.3d 777 (7th Cir. 2005) (ruling that appropriation act prohibition on the use of federal funds "to disclose to the public" certain ATF database records "prevents the agency…from acting on a request for disclosure "and that the act's provisions making such data "immune from legal process" prevents a court from utilizing a plaintiff-compensated special master to process such data).

D. **Exemption 4: Trade Secrets, and Commercial and Financial Records**. This exception balances and safeguards the interests of both the federal government and entities that submit commercial and financial information to the government.

1. Statutory language. The FOIA permits withholding records that are "trade secrets and commercial or financial information obtained from a person that are privileged or confidential."

2. Trade Secrets. There is a difference between the Trade Secrets Act and the FOIA's exemption for trade secrets.

a. For purposes of the FOIA, "Trade Secrets" has a narrow definition.

(1) "[A] secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either

innovation or substantial effort." Public Citizen Health Research Group v. FDA, 704 F.2d 1280 (D.C. Cir. 1983).

(2) The passage of time may not make trade secrets any less secret. Herrick v. Garvey, 298 F.3d 1184 (10th Cir. 2002) (upholding district court ruling that technical drawings and specification documents for 1935 airplane still retain commercial value and are protected by Exemption 4).

b. The Trade Secrets Act, 18 U.S.C. § 1905, defines secrets far more loosely. This act criminalizes the unauthorized disclosure of any data protected by Exemption 4. CNA Financial Corp. v. Donovan, 830 F.2d 1132 (D.C. Cir. 1987).

(1) Trade Secrets Act applies broadly to virtually all business information and prohibits agency disclosure except as "authorized by law."

(2) FOIA provides such "authority" to disclose business information only if it is nonexempt. CNA Fin. Corp., *supra*.

3. Commercial or financial information. Courts generally give these terms their "ordinary meanings" and reject more limiting definitions. *See* Public Citizen Health Research Group v. Food and Drug Administration, 704 F.2d 1280 (D.C. Cir 1983); s*ee also* Baker & Hostetler LLP v. U.S. Department of Commerce, 473 F.3d 312 (D.C. Cir. 2006) (information about lumber industry's "commercial strengths and challenges" even though they do not "reveal basic commercial operations…or relate to the income producing aspects of a business").

4. From a person. Person is defined as any individual or entity other than the Federal Government or one of its activities. Nadler v. FDIC, 92 F.3d 93 (2d Cir. 1996) (person includes individuals, partnerships, corporations, associations or public and private organizations other than an agency); Stone v. Export-Import Bank of United States, 552 F.2d 132 (5th Cir. 1977) (foreign government agency).

5. Privileged. Generally related to common law privileges, but rarely used as a basis for withholding. Sharyland Water Supply Corp. v. Black, 755 F.2d 397 (5th Cir. 1985); Indian Law Resource Center v. Department of the Interior, 477 F. Supp. 144 (D.D.C.1979).

6. Confidential. The Supreme Court examined the definition of confidential under Exemption 4 and overturned the standard that was applied for over 40 years. Where commercial or financial information is both customarily and treated as private by its owner and provided to the government under an assurance of privacy, the information is "confidential" within the meaning of Exemption 4. Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 915 (2019).

a. The first prong of the confidentiality analysis is whether the "commercial or financial information is both customarily and actually

treated as private by its owner." Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 915 (2019).

b. Upon finding the first prong of the confidentiality analysis to be satisfied, courts have taken differing approaches to the second prong – whether the government provided assurances that the information would be kept private. This is because the Supreme Court left open the question of whether this prong must additionally be satisfied. *See* Argus Leader Media, 139 S. Ct. at 2363.

(1) Unit prices are not [generally] confidential. *See, e.g.,* Pacific Architects & Eng'rs, Inc. v. Department of State, 906 F.2d 1345 (9th Cir. 1990); Acumenics Research & Technology v. Department of Justice, 848 F.2d 800 (4th Cir. 1988). The disclosure of government contract unit prices is a contentious issue.

(a) Government policy formerly required "submitter notice" in response to requests for contract unit prices, IAW Executive Order 12,600. 52 Fed. Reg. 23,781 (Jul. 23, 1987); *see also* 3 C.F.R. 235 (1988) *reprinted in* 5 U.S.C. § 552 note (1994). Submitters would then file "reverse FOIA" lawsuits to prevent the disclosure of unit prices as confidential commercial or financial information.

(b) In 1997, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council announced the change to Part 15 of the Federal Acquisition Regulation. FAR, 48 C.F.R. §§ 15.503(b)(iv), 15.506(d)(2), required disclosure of unit prices, upon request, in government contracts solicited after 1 January 1998. As a result, government policy no longer required submitter notice under EO 12600.

(c) Despite the best efforts of the Department of Justice and DoD, several courts have held that unit prices may be withheld under the FOIA. *See* Canadian Commer. Corp. v. Department of the Air Force, 514 F.3d 37 (D.C. Cir. 2008) (finding that line item pricing information involved in the option years of a maintenance contract must be protected); McDonnell Douglas Corp. v. Department of the Air Force, 375 F.3d 1182 (D.C. Cir. 2004) (finds that company has shown that disclosure of option prices and vendor pricing and handling factor, but not "over and above" prices, would likely cause substantial harm to its competitive position); McDonnell Douglas Corp. v. NASA, 180 F.3d 303 (D.C. Cir. 1999), *reh'g denied*, No. 98-5251 (D.C. Cir. Oct. 6, 1999) (finding line item price information from contract resulting from pre-1998 contract solicitation to be confidential under National Parks test); MCI Worldcom v. GSA, 163 F. Supp. 2d 28 (D.D.C. 2001) (FAR provisions cannot be read to authorize disclosure of information protected by Exemption 4 because authorizing statute, 41 U.S.C. § 253b(e)(3), prohibits disclosure of exempt info).

(d) Department of Justice policy again requires agencies to follow submitter notice procedures in response to requests for unit prices. On a case-by-case basis, agencies should determine the applicability of Exemption 4 to unit price requests. *See* U.S. Department of Justice, "Treatment of Unit Prices After McDonnell Douglas v. Air Force," FOIA Post, http://www.usdoj.gov/oip/foiapost/2005foiapost17.htm. The DoD Freedom of Information and Security Review (DFOISR) is expected to issue specific guidance. *See also* R&W Flammann GmbH v. United States, 339 F.3d 1320 (Fed Cir. 2003) (holding, in a pre-award bid protest case concerning unit prices contained in sealed bids –as distinct from prices contained in proposals – which were subject to the public opening requirement contained in a different FAR provision, that such bid prices "entered the public domain upon bid opening, and therefore…did not fall within Exemption 4 of FOIA").

(2) Unit prices and other items within an unsuccessful proposal are not releasable. 10 U.S.C. § 2305(g)(2) or 41 U.S.C. § 253b(m)(2).

7. How does agency determine what is confidential? *See* EO 12600 (June 23, 1987) and DoDM 5400.07, para. 5.2.d.(3).

8. Submitters can often be in a better position than the agency to answer questions relevant to an Exemption 4 inquiry (e.g., whether "information is both customarily and actually treated as private by its owner.") Although E.O. 12,600 speaks in language of "substantial competitive harm" as relevant legal test, and that test has been overruled, the submitter notice process is still entirely appropriate for agencies to continue to use when determining whether information is "confidential" under the test articulated in FMI v. Argus Leader (2019). Determining whether business information is exempt--notice of proposed release to the submitter of information — "Reverse FOIA"

a. Notify the submitter of the FOIA request and solicit its views as to whether the "information is both customarily and actually treated as private.

b. After reviewing submitter's comments, if the agency determines to disclose any information, it must advise the submitter of its rationale and inform it of the date it will make the disclosure. See NW. Coal. for Alternatives to Pesticides v. EPA, 254 F.Supp. 2d 125 (D.D.C. 2003) (upbraiding agency where submitter mailed redacted document to requester).

c. The agency rationale must be detailed and respond to each of the submitter's claims as it will constitute the "administrative record" that will support the agency's decision to release the requested information. Acumenics Research & Technology v. Department of Justice, 843 F.2d

800 (4th Cir. 1988) ("Reverse FOIA" case). *See* Federal Electric Corp. v. Carlucci, 866 F.2d 1530 (D.C. Cir. 1989) (agency failed to create an adequate agency administrative record).

d. Businesses that submit documents to the government may file suit under the Administrative Procedures Act (APA) to challenge an agency's decision to release documents pursuant to a FOIA request. Chrysler Corp. v. Brown, 441 U.S. 281 (1979) (discretionary release permissible only if not protected by Exemption 4, thereby "authorized by law"); Gulf Oil Corp. v. Brock, 778 F.2d 834 (D.C. Cir. 1985).

e. Standard of review of agency action under APA -- review on the administrative record using the arbitrary and capricious standard. Acumenics Research & Technology v. Department of Justice, 843 F.2d 800 (4th Cir. 1988); General Electric Co. v. NRC, 750 F.2d 1394 (7th Cir. 1984).

E. **Exemption 5: Privileged Memoranda & Internal Agency Communications**. The FOIA permits withholding records that are "inter-agency or intra-agency memorandums or letters which would not be available by law to a party . . . in litigation with the agency." Exemption 5 is limited to that information which would "routinely" or "normally" not be available to a party in litigation. FTC v. Grollier, 462 U.S. 19 (1983).

1. Threshold: Memoranda or communications must be "inter-agency or intra-agency."

a. "Inter- or intra-agency memorandums" may include communications with parties outside the government. Nat'l Institute of Military Justice v. Department of Defense, 512 F.3d 677 (D.C. Cir. 2008) (cert. denied 08-125 (Dec. 15, 2008)) (2- to-1 decision) (memoranda provided to DoD by outside experts for consideration in establishing regulations for terrorist trial commissions qualify under the D.C. Circuit's "consultant corollary").

b. Competing or conflicting interests may require disclosure of records of communications with "outside consultant." *See* Department of the Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1 (2001) ("intra-agency condition excludes, at the least, communications to or from an interested party seeking government benefit at the expense of other applicants").

2. Scope. Exemption 5 incorporates most common law discovery privileges.

a. Deliberative Process Privilege. Purpose--to encourage open, frank discussions between subordinates and superiors; protect against premature disclosure of proposed policies before they are adopted; and protect against public confusion that might result from disclosure of reasons and rationales that were not ultimately the grounds for the agency's action. Russell v. Department of the Air Force, 682 F.2d 1045 (D.C. Cir. 1982); Judicial Watch, Inc. v. United States Department of Justice, 102 F.Supp.2d 6 (D.D.C. 2000) (deliberative process privilege protects handwritten notes by the Attorney General which reflect distillations of issues that she

memorialized for later reference as part of her decision making process); Bilbrey v. Department of the Air Force, No. 00-0539 (W.D. Mo. Jan, 30, 2001) (protecting advice in two memoranda from wing commander to air force commander concerning nonjudicial punishment for requester charged with two counts of adultery and one of dereliction of duty; factual information in second memoranda used to rebut defense matters raised by requester ordered disclosed; that requester would have received the withheld information had he demanded a court-martial, and that he has a current need for the information, held irrelevant), *aff'd,* 20 Fed. Appx. 597 (8th Cir. 2001).

(1) Courts distinguish between "factual" and "deliberative" information. EPA v. Mink, 410 U.S. 73 (1973) (privilege does not generally protect purely factual matters).

(a) However, agency may withhold facts if they are "inextricably intertwined" with deliberative material. Ryan v. DOJ, 617 F.2d 781 (D.C. Cir. 1980); Jowett, Inc. v. Department of Navy, 729 F. Supp. 871 (D.D.C. 1989).

(b) Agency may also withhold facts if release would disclose the "deliberative process." Mead Data Central, Inc. v. Department of the Air Force, 566 F.2d 242 (D.C. Cir. 1977) (holding that "Exemption five is intended to protect the deliberative process of government and not just deliberative material . . . In some circumstances . . . the disclosure of even purely factual material may so expose the deliberative process within an agency that it must be deemed exempted by section 552(b)(5).")

(c) Deliberative documents and communications do not always have to flow from subordinates to superiors. Nat'l Wildlife Fed'n v. U.S. Forest Serv., 861 F.2d 1114 (9th Cir. 1988).

(2) Courts also distinguish between "predecisional" and "postdecisional" records.

(a) A document is predecisional if it was `prepared in order to assist an agency decisionmaker in arriving at his decision,' rather than to support a decision already made." Petroleum Info. Corp., 976 F.2d at 1434 (quoting Renegotiation Bd. v. Grumman Aircraft Eng'g Corp., 421 U.S. 168, 184 (1975)).

(b) Agency may withhold predecisional documents. NLRB v. Sears, 421 U.S. 132 (1975) (Deliberative process privilege can never apply to a final agency decision, but Exemption 5 incorporates the attorney-work privilege and documents setting strategy for the case); Lurie v. Department of the Army, 970 F. Supp. 19, 28 (D.D.C. 1997).

(c) Agency cannot withhold predecisional materials when final decision- maker "expressly adopts or incorporates them by

reference." NLRB v. Sears, 421 U.S. 132 (1975); Swisher v. Department of the Air Force, 660 F.2d 369 (8th Cir. 1981).

(d) Examples of the type of documents that might qualify as predecisional are "recommendations, draft documents, proposals, suggestions, and other subjective documents which reflect the personal opinions of the writer rather than the policy of the agency. Coastal States Gas Corporation v. Department of Energy, 617 F.2d 854, 866 (D.C. Cir. 1980).

(3) Under the FOIA Improvement Act of 2016, the deliberative process privilege no longer applies to records created 25 or more years prior to the date of the FOIA request.

b. Attorney Work-Product Privilege.

(1) Exempts materials "prepared in anticipation of litigation or for trial by or for [a] party or by or for that . . . party's representative (including the . . . party's attorney, consultant, . . . or agent)." Fed.R.Civ.P. 26(b)(3); FTC v. Grolier, 462 U.S. 19 (1983); Safecard Services, Inc. v. SEC, 926 F.2d 1197 (D.C. Cir. 1991). *See* Coleman v. U.S. Department of Justice, No. 02-79-A (E.D. Va. Oct. 7, 2002) (the privilege protects investigatory documents that contain "mental impressions, conclusions, opinions or legal theories" of the attorneys involved).

(2) Courts have recognized that the privilege extends to records prepared in anticipation of litigation even when no specific claim is pending. Schiller v. NLRB, 964 F.2d 1205 (D.C Cir. 1992) (holding that documents that provide tips on handling future litigation are covered by the work product privilege). *See also* Maine v. Department of the Interior, 298 F.3d 60 (1st Cir. 2002) (amended opinion) (concluding that court's earlier opinion which required that litigation be primary factor in creation of documents for which attorney work- product privilege was claimed, was in error). *But cf.* Jongeling v. Army Corps of Eng'rs, No. 02-1020 (D.S.D. Jan. 2, 2003) (attorney work-product privilege cannot be claimed as defendant agency has not shown that the records at issue were prepared "in anticipation of litigation" or "because of" the prospect of litigation; on in camera inspection).

c. Attorney-Client Privilege. The confidential communications from clients to the counsel made for the purpose of securing legal advice or services; and the communications from attorneys to their clients if the communications rest "on confidential information obtained from the client." In re Sealed Cases, 737 F.2d 94, 98-99 (D.C. Cir. 1984). Mead Data Central, Inc. v. Department of the Air Force, 566 F.2d 242 (D.C. Cir. 1977). *See also* Citizens Progressive Alliance v. United States Bureau of Indian Affairs, 241 F. Supp. 2d 1342 (D.N.M. 2002) (privileges not waived when DOJ attorney confidentially disclosed documents to the attorney for interveners because the "common interest privilege," an exception to the

inherent confidentiality requirement of the attorney-client privilege or the attorney work-product privilege, allows attorneys facing a common litigation opponent to exchange privileged communications and attorney work-product in order to adequately prepare a defense).

d. Government's Commercial Information Privilege. Federal Open Market Committee v. Merrill, 443 U.S. 340 (1979) (Exemption 5 incorporates privilege for commercially sensitive documents generated by the government); Morrison- Knudsen Co. v. Department of the Army, 595 F. Supp. 352 (D.D.C. 1984), *aff'd* 762 F.2d 138 (D.C. Cir. 1985) (table cite); Hack v. Department of Energy, 538 F. Supp. 1098 (D.D.C. 1992) (inter-agency cost estimates prepared by government for use in evaluating construction proposals submitted by private contractors).

e. Protection of Certain Confidential Witness Statements. United States v. Weber Aircraft Corp., 465 U.S. 792 (1984) (protecting witness statements given to military personnel in course of military air crash safety investigation); Ahearn v. Department of the Army, 583 F. Supp. 1123 (D. Mass. 1984) (protecting statements made in Inspector General investigations).

f. Presidential Communications Privilege. Loving v. Department of Defense, 550 F.3d 32 (D.C. Cir. 2008) (TJAG's analysis and recommendation to the Secretary of the Army for transmittal to the president for him to determine whether to approve requester's death sentence; ruling this privilege, unlike deliberative process privilege, protects facts; holding that privilege's requirement that the communication must be reviewed by the president or solicited by his immediate advisors is satisfied by the "solicitation" for the TJAG opinion in R.C.M. 1204(c)(2)).

F. **Exemption 6: Protection of Personal Privacy**. FOIA permits withholding records that are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;"

1. Threshold: Record must be from a "personnel and medical files and **similar files**."

a. "Personal and medical files" are normally easy to identify. Includes military members' OMPF, local unit personnel files, and military medical records.

b. What are "similar files?" Department of State v. Washington Post, 456 U.S. 595 (1986) ("similar files" provision extends to any information of a "personal" nature, such as ones citizenship); Perlman v. U.S. Department of Justice, 312 F.3d 100 (2d Cir. 2002) (report of investigation is a "similar file" because it is a "detailed Government record"); New York Times Co. v. NASA, 920 F.2d 1002 (D.C. Cir. 1990) (holding that voice recording of the Challenger astronauts is a "similar file" for purposes of FOIA Exemption 6).

c. Information must identify a specific individual; records which identify a

group of individuals do not qualify for Exemption 6 withholding unless the information is attributable to all members of the group. Arieff v. Department of the Navy, 712 F.2d 1462 (D.C. Cir. 1983) (list of drugs used by some within a 600-member group); Na Iwi O Na Kupuna v. Dalton, 894 F. Supp. 1397 (D. Haw. 1995) (records pertaining to large group of ancient human remains subject to FOIA, Congress intended Exemption 6 to only "protect the privacy of living members of contemporary society").

2. The balancing test: whether disclosure "would constitute a clearly unwarranted invasion of privacy." Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989). *See also* Bibles v. Oregon Natural Desert Association, 519 U.S. 355 (1997).

a. Identifying the privacy interest to be balanced.

(1) The privacy rights of the deceased is a settled issue.

(a) Deceased persons have no privacy rights. National Archives & Records Administration v. Favish, 541 U.S. 197 (2004) (unanimous ruling that death-scene photographs can be withheld from the public, and from media exploitation, "to protect…the personal privacy of family members against the uncontrolled release of information"; *See also*; Na Iwi O Na Kupuna v. Dalton, *supra*. (Reverse FOIA suit).

(b) Next-of-kin of deceased persons may have, in certain situations, a colorable privacy interest in "time-of-death" records. New York Times Co. v. NASA, 920 F.2d 1002 (D.C. Cir. 1990) (*en banc*) (voice recordings of space shuttle Challenger astronauts; next-of-kin may have, in rare situations, a colorable privacy interest). *But cf.* Outlaw v. Department of the Army, 815 F.Supp. 505 (D.D.C. 1993) (agency unable to determine, in connection with murderer's request for death scene photographs, whether murdered First Sergeant had any surviving next of kin 25 years after his death).

(2) Corporations and business associations do not generally have protectable privacy interests. *See* Sims v. CIA, 642 F.2d 562, 572 n.47 (D.C. Cir. 1980). However, persons associated with small businesses, partnerships, and closely held corporations may have protectable interests in their entrepreneurial information. Doe v. Veneman, 230 F.Supp. 2d 739 (W.D. Tex. 2002) ("reverse" FOIA action brought by "incorporated" ranchers who entered into agreements with the government on the use of "anti-wolf livestock protection collar" who seek protection of their own identities, court protects the identities of entrepreneurial entities who have signed the agreements because the agency was making an "overly technical distinction" between individual and business), *aff'd in pertinent part on other grounds*, 380 F.3d 807 (5th Cir. 2004).

(3) "Something, even a modest privacy interest, outweighs nothing every time." Nat'l Association of Retired Federal Employees v. Horner, 879 F.2d 873 879 (D.C. Cir. 1989).

(4) Associated Press v. Department of Defense (2nd Cir. Jan. 5, 2009) (holding that identifying information of Guantanamo Bay detainees in records documenting abuse allegations and identifying information of detainees' family members in letters submitted to the government are exempt from FOIA disclosure under Exemptions 7(C) and 6 respectively).

b. Identifying the public interest in disclosure. The Reporters Committee decision has limited the concept of public interest under the FOIA to the "core purpose" for which Congress enacted it: to "[shed] light on an agency's performance of its statutory duties." Information that does not directly reveal the operations or activities of the federal government "falls outside the ambit of the public interest that the FOIA was enacted to serve." If records are not informative on the operations and activities of the government, there is no public interest in their release. For an example of a court finding a qualifying public interest see Cochran v. United States, 770 F.2d 949 (11th Cir. 1985) (disclosure of nonjudicial findings and discipline imposed on Army major general for misuse of government personnel and facilities held proper) (Privacy Act wrongful disclosure suit).

3. Application of the balancing test.

a. Articulate the privacy interest involved. [Note the **"heightened interest in the personal privacy of DoD personnel"** resulting from terrorist activity likely to weigh heavily in favor or protection. *See* 9 November 2001, DoD guidance, at Appendix B]; see also Kimmel v DoD, 2006 U.S. Dist. LEXIS 14904 (D.D.C. Mar. 31, 2006) (protecting "names of civilian personnel below the level of office director and military personnel below the rank of colonel" in documents relating to congressional request that the President advance Rear Admiral Kimmel to the rank of Admiral; finding disclosure of those names would not shed light on the operations and activities of DoD; ruling that the court "has no reason to question" the DoD policy expressing "concern that employees of DoD could become targets of terrorist assaults"). Long v. OPM, No. 05-1522, 2007 U.S. Dist. LEXIS 72887 (N.D.N.Y. Sept. 30, 2007) (An employee's name and duty station are personal in nature and do not relate to the employee's performance of public duties. Disclosure of lists of names does not, by itself, shed light on agency activities.)

b. Articulate the public interest involved.

c. Strike the balance.

d. Examples. FLRA v. DoD, 510 U.S. 487 (1994) (a leading case delineating the "core interests" of FOIA; thorough balancing of interests

analysis); Department of State v. Ray, 502 U.S. 164 (1991) (privacy interest of Haitian deportees in their names and addresses outweighs any public interest that might be served by disclosure); Judicial Watch, Inc. v. United States, 84 F.App'x 335 (4th Cir. 2004) (protecting the names of lower-level IRS employees because disclosure would not shed light on the activities of the IRS); Sherman v. Department of the Army, 244 F.3d 357 (5th Cir. 2001) (protecting Social Security numbers in post-1968 award orders; though Army in past released some SSNs of service members, such disclosures do not waive privacy interests because only individuals can waive their privacy interests); Sheet Metal Workers Int'l Ass'n. v. United States Air Force, 63 F.3d 994 (10th Cir. 1995) (Sheet Metal Workers union engaged in "Davis-Bacon" monitoring--release of payroll records with names and addresses of workers employed on government contracts constitutes a clearly unwarranted invasion of personal privacy); McCutchen v. HHS, 30 F.3d 183 (D.C. Cir. 1994) (names of persons exonerated by investigation protected from disclosure); Providence Journal Co. v. Department of the Army, 981 F.2d 552 (1st Cir. 1992) (the higher the rank, the greater the public interest might be in release of agency record concerning disciplinary action); Homer J. Olsen, Inc. v. U.S. Department of Transp., 2002 U.S. Dist. LEXIS 23292 (N.D. Cal. Dec. 2, 2002) (disclosure of names of contractor and subcontractor employees "would constitute a clearly unwarranted invasion of personal privacy"); Chin v. Department of the Air Force, No. 97-2176 (W.D. LA June 24, 1999) (privacy outweighed the public interest in withholding of identities in general request for fraternization investigations); Mueller v. Department of the Air Force, 63 F. Supp. 2d 738 (E.D. Va. 1999) (denial of request for dismissed non-judicial punishment proceeding documents because public interest was minimal and would shed little light on Air Force's overall conduct).

4. "Categorical Balancing" and Privacy Glomarization. Agency can refuse to confirm or deny categories of records; however, application must be consistent. *See* Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989); Beck v. Department of Justice, 997 F.2d 1489 (D.C. Cir. 1993); DoDM 5400.07, para. 5.1.f.(2).

G. **Exemption 7: Law Enforcement Records**. Exempts from disclosure any record or information compiled for law enforcement purposes, the disclosure of which could reasonably be expected to result in any of six specified harms.

1. Threshold. Record must be compiled for a law enforcement purpose.

a. Courts have distinguished between agencies whose primary purpose is law enforcement and agencies with both law enforcement and administrative functions. *See* Jefferson v. Department of Justice, 284 F.3d 172 (D.C. Cir. 2002) (ruling agencies must distinguish between records based on "allegations that could lead to civil and criminal sanctions" and records "maintained in the course of general oversight of government employees").

(1) Agency whose primary function is not law enforcement (e.g., DoD's

primary function is war-fighting, not law enforcement) must establish that particular records at issue involved the enforcement of a statute or regulation within its authority. Jefferson v. Department of Justice, *supra* (DoJ's Office of Professional Responsibility has mixed functions, function related to collection of evidence for potential prosecution of attorney sufficiently related to a law enforcement function); Tax Analysts v. IRS, 294 F.3d 71 (D.C. Cir. 2002) (district court erred when it ruled that IRS does not compile information for law enforcement purpose).

(2) The exemption covers all law enforcement records, both "investigatory and non-investigatory materials. Tax Analysts v. IRS, *supra.*

b. Record must have a law enforcement purpose.

(1) Information that was originally compiled for law enforcement purposes, but later summarized in a new document not prepared for law enforcement purposes, is protected under the exemption. Abramson v. FBI, 456 U.S. 615 (1982).

(2) Exemption will protect non-law enforcement records that are "recompiled" for law enforcement purposes. John Doe Agency v. John Doe Corporation, 493 U.S. 146 (1989).

2. An agency *may* withhold law enforcement records under this exemption, but only to the extent disclosure:

"(A) could reasonably be expected to interfere with enforcement proceedings,

"(B) would deprive a person of a right to a fair trial or an impartial adjudication,

"(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,

"(D) could reasonably be expected to disclose the identity of a confidential source. . . in a criminal or national security investigation . . . or information furnished by a confidential source,

"(E) would disclose techniques and procedures or would disclose guidelines for law enforcement investigations or prosecutions if disclosure could reasonably be expected to risk circumvention of the law, or

"(F) could reasonably be expected to endanger the life or physical safety of any person."

3. Exception 7(A) does not require an agency to make a specific showing

within the context of a particular case.

a. Agency may demonstrate that the disclosure of certain classes of documents would have the effect of interfering with agency enforcement. NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214 (1978).

b. Agency may rely upon Exemption 7(A) to exempt records only while a law enforcement proceeding [includes prosecution] is pending. *See* Maydak v. Department of Justice, 218 F.3d 760 (D.C. Cir. 2000) (refusing to allow agency to rely on exemptions not previously "substantiated" after it withdrew reliance upon Exemption 7(A) due to change in underlying circumstances; ordering disclosure of grand jury records, attorney work-product, and law enforcement records without redaction), *reh'g en banc denied*, No. 98-5492 (D.C. Cir. Oct. 30, 2000), *stay granted* (D.C. Cir Nov. 29, 2000), *cert. denied*, 121 S. Ct. 2591 (2001). *See also* Ctr. for Nat'l Sec. Studies v. United States Department of Justice, 331 F.3d 918 (D.C. Cir. 2003) (upholding withholding of the identities of detainees held during the post-9/11 terrorist investigation, because disclosure "would give terrorist organizations a composite picture of the government investigation" and thus enable them to impede it through "counter-efforts.").

4. Use of Exemption 7(B) is designed to prevent pre-trial publicity that would deprive a person of a fair trial.

a. Use of this exemption dependent upon a two-part test: a pending or imminent proceeding and determination that disclosure more probably than not would interfere with fairness.

b. There are few cases in this area. *See* Dow Jones Co., Inc. v. FERC, 219 F.R.D. 167 (C.D. Cal. 2002) (agency has not shown that any trial or adjudication is "pending or truly imminent" or that disclosure would generate pretrial publicity that could deprive the companies or their employees of their right to a fair trial).

5. Exemption 7(C) protects the personal privacy of individuals named in law enforcement files. *See* SafeCard Serv. v. SEC, 926 F.2d 1197 (D.C. Cir. 1991).

a. Privacy protections standards are greater under 7(C) than Exemption 6 ("reasonably be expected to constitute an unwarranted invasion of personal privacy" versus "clearly unwarranted invasion"). Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

b. Protects the names of both witnesses and investigators. *See* Palacio v. Department of Justice, No. 02-5247, 2003 U.S. App. LEXIS 1804 (D.C. Cir. Jan. 31, 2002) (*per curiam*) (identities of suspects, witnesses, and investigators properly withheld under Exemption 7(C)); Rugiero v. U.S. Department of Justice, 257 F.3d 534 (6th Cir. 2001) (protects the identities of government employees and investigators contained in DEA's

investigatory files); Davis v. United States Department of Justice, No. 00-2457 (D.D.C. Mar. 21, 2003) (protects information that would identify FBI Special Agents and support personnel, other federal employees, third parties, informants, subjects of investigative interest, bank personnel, and state, local, federal, and foreign law enforcement personnel). *See also* Billington v. United States Department of Justice, 11 F.Supp. 2d 45 (D.D.C. 1998) (individual who admitted that he was an FBI informant possesses a diminished privacy interest under Exemption 7(C), but has not waived its protection) *aff'd in pertinent part*, 233 F.3d 581 (D.C. Cir. 2000).

c. Glomar responses to targeted requests are appropriate. U.S. Department of Justice v. Reporters Comm. For Freedom of the Press, 489 U.S. 749 (1989) (ruling that FBI properly refused to confirm or deny whether it had a "rap sheet" on an alleged member of organized crime); Oguaju v. United States, 288 F.3d 448 (D.C. Cir. 2002) (Marshall Service properly refused to confirm or deny the existence of records regarding an escapee-turned-informant/ witness at the requester's trial); Pusa v. FBI, 31 F.App'x 567 (9th Cir. 2002) (FBI properly refused to confirm or deny existence of records pertaining to communications between FBI and certain named third parties); Taylor v. Department of Justice, 257 F.Supp. 2d 101 (D.D.C. 2003) (holding there is no public interest in disclosure of third-party information that might assist a convict in challenging his conviction; FBI properly refused to confirm or deny the existence of records on living persons). *See also*, DoDM 5400.07, para. 5.2.g.(1)(c).

d. Exemption 7(C) may protect privacy of the close survivors of the deceased from disclosure of facts concerning his death. NARA v. Favish, 541 U.S. 157 (2004) (protecting privacy interests of close family members from the pain that would flow from the death scene photographs of Deputy White House Counsel Vincent Foster); Badhwar v. U.S. Department of the Air Force, 829 F.2d 182 (D.C. Cir. 1987) (disclosure of autopsy reports "might shock the sensibilities of surviving kin"); NY Times v. NASA, 782 F.Supp. 628 (D.D.C. 1991) (withholding audiotape of voices of Space Shuttle *Challenger* astronauts recorded immediately before their deaths, to protect family members from pain of hearing final words of loved ones).

e. In a reverse FOIA case, the Supreme Court ruled that a corporation has no personal privacy interest in agency's investigation of its overcharging of schools for telecommunication services; observing that "[a]djectives typically reflect the meaning of corresponding nouns, but not always. Sometimes they acquire distinct meanings of their own" and in this case the "it" would not be reasonable to interpret the adjective "personal" to reflect the meaning of "person." The Supreme Court rejected the argument that the term "person" included a corporation in the phrase "personal privacy" and closed by saying "[w]e trust that AT&T will not take it personally." FCC v. AT&T, Inc., 131 S. Ct. 1177 (2011).

f. Exemption 7(C) may protect privacy by protecting identities of agency supervisors at levels equivalent to GS-14 and GS-15 disciplined for viewing

pornography during work hours; "disclosure in this case is not limited to the reputational embarrassment of having misused government property on official time but rather extends to the embarrassment resulting from public knowledge that the conduct was of a sexual nature" and ruling that the disclosure of the names is not necessary to show the agency's "operations and activities" in light of the extensive release of the IG's report. Steese, Evans & Frankel v. SEC, No. 10-1071, Dist. LEXIS 129401 (D. Col. Dec. 7, 2010).

6. The purpose of Exemption 7(D) is to ensure that "confidential sources are not lost through retaliation against the source for past disclosure or because of source's fear of future disclosure." Brandt Construction v. Environmental Protection Agency, 778 F.2d 1258 (7th Cir. 1985).

a. Protects source's identity whenever he provides information under either an express promise of confidentiality or "under circumstances from which such an assurance could reasonably be inferred." *See* U.S. Department of Justice v. Landano, 508 U.S. 165 (1993); Rosenfeld v. Department of Justice, 57 F.3d 803 (9th Cir. 1995). *But see* Cooper Cameron Corp. v. U.S. Department of Labor, 280 F.3d 539 (5th Cir. Tex. 2002) (ordering disclosure of OSHA witness statements; finding no express promises of confidentiality despite declarant's statement that agency manual requires express promises to be given; implicitly and aberrationally ruling that circumstances giving rise to an implied promise of confidentiality can occur in a criminal investigation only).

b. The term "confidential source" is provided wider definition than limited meaning within criminal matters. This exemption is not limited to criminal witnesses and victims, rather protections are afforded to broad spectrum of individuals and institutions, excluding federal employees acting in their official capacity. *See* Retail Credit Company v. Federal Trade Commission, No. 75-0895, 1976 WL 1206 (D.D.C. 1976).

7. Exemption 7(E) provides protections similar to what was previously "High 2." *See* Coastal Delivery Corp. v. United States Customs Serv., 272 F.Supp.2d 958 (C.D. Cal. 2003) (holding agency properly withheld records of Customs Service examinations conducted at the Los Angeles/Long Beach seaport "because terrorists . . . could use the information to discover the rate of inspection and then direct their containers to vulnerable ports."); *reconsideration denied* id. at 966-68 (C.D. Cal. 2003); *appeal dismissed voluntarily*, No. 03-55833 (9th Cir. Aug. 26, 2003).

8. Exemption 7(F) permits the withholding of records necessary to protect the physical safety of a wide range of individuals.

a. No balancing test is required. *See* Living Rivers, Inc. v. United States Bureau of Reclamation, 272 F.Supp.2d 1313 (D. Utah 2003) (withholding of "inundation maps" of potential flood zones beneath Hoover and Glen Canyon Dams because disclosure "could aid in carrying out a terrorist attack" that

"could reasonably place at risk the li[ves] or physical safety" of area residents; court held maps were compiled "in direct relation to" a governmental law enforcement function). *But see* ACLU v. DoD, 06-3140, 2008 WL 4287823 (2d Cir. Sept. 22, 2008) (affirming disclosure order of 21 photographs with identity redacted under Exemption 7(c), showing mistreatment of detainees, even though court accepted that their release "could reasonably be expected to incite violence against United States troops, other Coalition forces, and civilians in Iraq and Afghanistan"; ruling that government's contention that "any individual" encompasses a person identified as belonging to of [sic] a population of national size would, if accepted, circumvent the limitation imposed by the phrase "could reasonably be expected to endanger.")

b. The agency must only show a reasonable likelihood of physical danger to withhold information. L.A. Times Common's, LLC v. Department of the Army, 442 F.Supp.2d 880 (C.D.Cal. 2006) (applying Exemption 7(F) where disclosure of private security contractor company names could endanger the life or safety of many individuals). Ctr. for Nat'l Sec. Studies v. U.S. Department of Justice, 215 F.Supp.2d 94 (D.D.C. 2002) (disclosure of the dates and locations of arrest, detention, and release of post-September 11th detainees would make detention facilities and their occupants vulnerable to retaliatory attacks), *rev'd in other part, aff'd in part on other grounds and remanded*, 331 F.3d 918 (D.C. Cir. 2003).

H. **Exemption 8: Financial Institutions Information**. Exemption 8 is rarely used within the DoD. For more information see DoJ FOIA Guide.

I. **Exemption 9: Geological and Geophysical Information**. Exemption 9 is rarely used within the DoD. For more information see DoJ FOIA Guide.

VII. EXCLUSIONS.

A. The FOIA amendment of 1986 provided a new mechanism by which the government could protect limited sensitive law enforcement records. These exclusions permit law enforcement officials to treat agency records as if they were not subject to the FOIA. Unlike normal FOIA responses in which the agency was required to either acknowledge the existence of records or provide a Glomar response, in cases involving exclusions, the agency merely responds that there are no records responsive to the request.

1. **Exclusion 1**. Investigation or proceedings involving possible criminal law violation, and subject unaware of pendency of investigation or proceedings, and disclosure of existence of records could reasonably be expected to interfere with enforcement proceedings.

2. **Exclusion 2**. Informant records maintained under informant's name or identifier, and maintained by a criminal law enforcement agency, unless informant's status as an informant has been officially confirmed.

3. **Exclusion 3**. Records maintained by FBI, and pertaining to foreign intelligence or counterintelligence, or international terrorism,

and existence of records is classified.

VIII. CONCLUSION.

"A popular government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or, perhaps, both." - Pres. James Madison, August 4, 1822.

"We seek a free flow of information . . . we are not afraid to entrust the American people with unpleasant facts, foreign ideas, alien philosophies, and competitive values." - Pres. John F. Kennedy, February 1962.

“The Freedom of Information Act (FOIA) is the embodiment of the public’s right to know about the activities of its government. . . . Under FOIA, those seeking information are no longer required to show a need for information; the “need to know” standard has been replaced by a “right to know” doctrine. The burden of proof for why certain information should be kept secret now falls on the government.” - A Citizen’s Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records, published by the House Committee on Oversight and Government Reform, September 2012.

CHAPTER B

THE PRIVACY ACT

5 USC § 552a

Outline of Instruction

I. REFERENCES.

A. Primary.

1. The Privacy Act of 1974, 5 U.S.C. § 552a, *as amended*.

2. Privacy Act Implementation, Office of Management and Budget, 40 Fed. Reg. 28948 (9 July 1975), *as amended*; 40 Fed. Reg. 56741 (4 December 1975).

3. OMB Guidelines, 51 Fed. Reg. 18,982, 18,985 (1986).

4. Dep't of Defense Instruction 5400.11, DoD Privacy and Civil Liberties Programs (29 January 2019).

5. Dep't of Defense Regulation No. 5400.11-R, Privacy Program (14 May 2007).

6. Army Regulation 25-22, The Army Privacy Program (22 December 2016).

7. Air Force Instruction 33-332, The Air Force Privacy and Civil Liberties Program (10 March 2020).

8. Secretary of the Navy Instruction 5211.5F, Department of the Navy Privacy Program (20 May 2019).

B. Secondary.

1. Overview of the Privacy Act of 1974, a Department of Justice publication; available at http://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

2. Defense Privacy and Civil Liberties Office Web Page, provides current Privacy Act System of Records Notices and other Privacy Act guidance and information; available at http://dpcld.defense.gov/Privacy.aspx.

3. Defense Privacy Board Advisory Opinions; available at http://dpcld.defense.gov/Privacy/AuthoritiesandGuidance.aspx

4. Service specific resources available online.

a. Army: https://www.rmda.army.mil/privacy/RMDA-PO-Division.html

b. Navy: http://www.doncio.navy.mil/tagresults.aspx?ID=36

c. Marine Corps: http://www.hqmc.marines.mil/Agencies/USMCFOIA/USMCPrivacyAct.aspx

d. Air Force: http://www.privacy.af.mil/

e. Coast Guard: https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6/The-Office-of-Information-Management-CG-61/FOIA-Library/

II. INTRODUCTION.

A. History of the Act. The Privacy Act of 1974 provides safeguards for the protection of records the Federal government collects on United States citizens or lawfully admitted permanent residents. It was passed in great haste during the final week of the Ninety-Third Congress after the illegal surveillance and investigation of individuals were exposed during the Watergate scandal. Due in part to its hasty enactment, no conference committee was convened to reconcile differences in the bills passed by the House and Senate. Instead, staffs of the respective committees--led by senators Ervin and Percy, and congressmen Moorhead and Erlenborn--prepared a final version of the bill that was ultimately enacted. The original reports are thus of limited utility in interpreting the final statute. The more reliable legislative history consists of a brief analysis of the compromise amendments--entitled "Analysis of House and Senate Compromise Amendments to the Federal Privacy Act"--prepared by the staffs of the counterpart Senate and House committees and submitted in both the House and Senate in lieu of a conference report. *See* 120 Cong. Rec. 40,405-09, 40,881-83 (1974), *reprinted in* Source Book on Privacy (1976) at 858-68, 987-94.

B. Policy Objectives. "Broadly stated, the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them." Overview of the Privacy Act (July 2015), 4. The Act addresses four major policy objectives:

1. Restrict disclosure of personal information maintained by agencies;

2. Allow individuals access to records about themselves;

3. Allow individuals to amend records about themselves; and,

4. Establish fair collection, maintenance and dissemination practices.

III. SCOPE OF THE ACT.

A. Generally applicable to agency records within a "System of Records." Manuel v. Veterans Administration Hospital, 857 F.2d 1112 (6th Cir. 1988).

B. Key Definitions.

1. "Agency" means "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President[*]), or any independent regulatory agency."

a. Privacy Act adopts the FOIA definition. 5 U.S.C. § 552a(a)(1) incorporates 5 U.S.C. § 552(f).

b. * The Office of the President and those organizations within the Executive Office of the President whose function is limited to advising and assisting the President are excluded from the definition of agency.

c. Government contractors and their employees are covered by the civil and criminal penalties of the Act, if provided for by the contract. 5 U.S.C. § 552a(m).

2. "Individual" means "any citizen of the United States or an alien lawfully admitted for permanent residence" in the U.S. 5 U.S.C. § 552a(a)(2).

a. Definition is far more restrictive than the FOIA's definition of "any person."

b. Does not include deceased individuals. Crumpton v. U.S., 843 F. Supp. 751 (D.D.C. 1994), *aff'd on other grounds*, 59 F. 3d 1400 (D.C. Cir. 1995). Likewise, neither surviving family members nor executors are specifically granted Privacy Act rights. *See* OMB Guidelines, 40 Fed. Reg. 28,948, 28,951 (11975). *But cf.* NARA v. Favish, 541 U.S. 157 (2004) (ruling that surviving relatives have a FOIA-recognized privacy interest in scene-of-death photos of their close relative).

c. Does not include corporations or business enterprises. Falwell v. Executive Office of the President, 158 F.Supp. 2d 734, 736 n.3 (W.D. Va. 2001) (plaintiff may make personal request under the Act, but Falwell's corporate alter-egos are not individuals as defined under the law); St. Michael's Convalescent Hospital v. California, 643 F.2d 1369 (9th Cir. 1981).

d. Privacy Act rights are personal to the individual and cannot be derivatively asserted by others. *See* Sirmans v. Caldera, 27 F. Supp. 2d 248 (D.D.C. 1998) (plaintiffs "may not object to the Army's failure to correct the records of other officers"); Abramsky v. U.S. Consumer Products Safety Comm'n., 478 F. Supp. 1040 (S.D.N.Y. 1979) (union president cannot compel release of records pertaining to employee's termination).

e. **Note**: Parents of minor children and guardians of incompetents may act on behalf of that individual. 5 U.S.C. § 552a(h). The OMB Guidelines also note that minors are also authorized to independently exercise their Privacy Act rights.

f. Entrepreneurial information. Sole proprietors are not "individuals" under OMB's view. OMB Guidelines 40 Fed. Reg. at 28,951. The cases are split 6-to-2 against OMB's views. *Compare, e.g.,* Scarbough v. Harvey, 493 F. Supp. 2d 1 (D.D.C., 2007) (rejecting distinction) *with* Shermco Indus. v. Sec'y of the U.S. Air Force, 452 F.Supp. 306 (N.D. Tex. 1978) (accepting distinction).

3. "Maintain" means to maintain, collect, use, or disseminate. § 552a(a)(3).

4. "Record" means "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or other identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4).

a. As a general rule, the threshold requirement is that the information must contain his name or otherwise identify an individual. Pierce v. U.S. Dep't of Air Force, 512 F. 3d 184 (5th Cir. 2007) (ruling that report of investigation summary, which refers to all personnel by job position rather than name, and contains no dates, is not a record). However, there are three jurisdictional differences in the manner in which courts determine whether a record is "about" an individual under the Act.

(1) Some jurisdictions require only that the record "**be about**" the subject of the record. *See* Unt v. Aerospace Corp., 765 F.2d 1440 (9th Cir. 1985) (letters written by appellant did not discuss appellant personally, therefore, they were not "records" subject to restrictive disclosure within the meaning of the Act).

(2) Some jurisdictions require the record **to both identify and be about** a subject. *See* Tobey v. NLRB, 40 F.3d 469 (D.C. Cir. 1994) (NLRB's computerized unfair labor practice case tracking system was not a system of records about individuals of which notice was required in the Federal Register despite the presence of the identity of the field examiner within the records).

(3) Some jurisdictions have a very broad definition of a record that includes **any information that identifies a subject and any personal characteristic**. *See* Bechhoefer v. Dep't of Drug Enforcement, 209 F.3d 57 (2d Cir. 2000) (appellant's letter, on letterhead including both his name and address, satisfied statutory definition of record).

b. In unsettled jurisdictions, the safest course is to follow the Bechhoefer definition.

5. A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying particular assigned to the individual. § 552a(a)(5). Manuel v. VA, 857 F.2d 1112 (6th Cir. 1988); Crumpton v. U.S., 843 F. Supp. 751 (D.D.C. 1994), *aff'd on other grounds*, 59 F. 3d 1400 (D.C. Cir. 1995).

a. The actual method of retrieval is the key to whether a record is within a system of records. Henke v. United States Dep't of Commerce, 83 F.3d 1453 (D.C. Cir. 1996) (holding that the test is whether the information is actually retrieved, not retrievable, by use of the individual's name or identifier); Yonemoto v. VA, No. 06-00378, 2007 WL 1310165 (D. Haw. May 2, 2007) (ruling that agency's e-mail archives are not a system of records; finding that "[j]ust because an agency is capable of retrieving the information,

and just because it does so to comply with a FOIA request, does not mean that the information is maintained in a Privacy Act 'system of records'"; such a manner of retrieval is not the "actual practice of the VA").

b. The technical definition of “system of records” makes coverage under the Act dependent upon the method of retrieval rather than the contents of the record. Consequently, there are critics who argue that this renders the Act subject to agency abuse. *See* U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society, (1977).

c. Personal notes – Treated the same as under the FOIA. Hudson v. Reno, 130 F.3d 1193 (6th Cir. 1997) (supervisor’s notes about plaintiff’s misconduct which were kept in a locked drawer and labeled the “First Assistant’s” files do not fall within this definition). *See also* Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 38:

> (1) “Personal notes of unit leaders or office supervisors concerning subordinates ordinarily are not records within a system of records governed by the Privacy Act. The Act defines ‘system of records’ as a ‘group of any records under the control of any agency…from which information is retrieved by the …[individual’s] identifying particular…’ [citation omitted]…Personal notes that are *merely an extension of the author’s memory*, if maintained properly, will not come under the provisions of the Privacy Act or the Freedom of Information Act [citation omitted] (emphasis added).” *Id*.
>
> (2) “To avoid being considered agency records, personal notes must meet certain requirements. *Keeping notes must be at the sole discretion of the author*. Any requirement by superior authority, whether by oral or written directive, regulation or command policy, likely would cause the notes to become official agency records. *Such notes must be restricted to the author’s personal use as memory aids*. *Passing them to a successor or showing them to other agency personnel would cause them to become agency records* (emphasis added). Chapman v. National Aeronautics and Space Administration, 682 F.2d 526 (5th Cir. 1982).”
>
> (3) “Even if personal notes do become agency records, they will not be within a system of records and subject to the Privacy Act unless they are retrieved by the individual’s name or other personal particular. Thus if they are filed only under the matter in which the subordinate acted or in a chronological record of office activities, the Privacy Act would not apply to them. However, [they] would be subject to disclosure under the FOIA.” Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 38.

(4) "Individuals who maintain personal notes about agency personnel should ensure their notes do not become records within systems of records. Maintaining a system of records without complying with the Privacy Act system notice requirement could subject the individual to criminal charges and a $5,000.00 fine. [citation omitted]." *Id. See also* Johnston v. Horne, 875 F.2d 1415 (9th Cir. 1989); Kalmin v. Dep't of Navy, 605 F. Supp. 1492 (D.D.C. 1985).

(5) An agency may incorporate personal notes into agency records if it does so in a timely manner. *Compare* Chapman v. NASA, 682 F.2d 526 (5th Cir. 1982) ("Act did not prohibit taking and keeping private notes by a supervisor. However, when the notes were no longer kept private and were used to evaluate plaintiff, they had to be maintained consistent with the Act") *with* Thompson v. Dep't of Transportation, 547 F. Supp. 274 (D. Fla. 1982) (timeliness requirement met where materials upon which adverse disciplinary action is based are placed in the appropriate system of records contemporaneously with or within a reasonable time after an adverse disciplinary action is proposed).

(6) *See* Johnson v. Horne, 875 F.2d 1415 (9th Cir. 1989) (supervisor's private notes about an employee not covered under Privacy Act because they are not agency records); Bowyer v. Dep't of the Air Force, 804 F.2d 428, 431-31 (7th Cir. 1986) (same); Boyd v. Secretary of the Navy, 709 F.2d 684, 686-87 (11th Cir. 1983) (same), *cert. denied,* 104 S. Ct. 709 (1984).

6. "Disclosure." The general prohibition is quite broad. "No agency shall disclose any record which is within a system of records by any means of communication to any person . . ." 5 U.S.C. § 552a(b).

a. Consent may **not** be implied.

b. Verbal reports of information maintained within a system of records may constitute an improper disclosure.

IV. PUBLIC NOTICE OF SYSTEMS OF RECORDS.

A. Publication Requirement. Public notice must appear in the Federal Register. 5 U.S.C. § 552a(e)(4).

1. No longer an annual requirement. However, advance notice to Congress and OMB is required for any new or altered system of records. 5 U.S.C. § 552a(r).

2. Publication in the Federal Register of any new routine use is required at least 30 days prior to use under (e)(4)(D) to provide an opportunity for public comment. 5 U.S.C. § 552a(e)(11).

3. There are both agency-specific and government-wide system notices. As a general rule, DOD and DOD components publish military-specific system notices. For a complete list of the DOD's Privacy Act System of Records Notices, as well as links to all government wide systems notices, see http://dpcld.defense.gov/Privacy/SORNs.aspx.

B. Contents of a system notice. 5 U.S.C. § 552a(e)(4).

1. Name and location of the system;

2. Categories of individuals on whom records are maintained;

3. Categories of records maintained in the system;

4. Each routine use of the records, including categories and purpose of users;

5. Policies and practices regarding storage, retrieval, access, retention, and disposal of records within the system;

6. Title and business address of the responsible agency official;

7. Procedures regarding individual's right to notification upon request;

8. Procedures whereby an individual can be notified at his request how he can gain access to any record retaining to him and how he can contest its contents; and,

9. Categories of sources of records in the system.

V. COLLECTION AND MAINTENANCE OF INFORMATION

A. Collect only relevant and necessary information to accomplish an agency purpose as defined by statute or Executive Order. 5 U.S.C. § 552a(e)(1).

B. Collect information to greatest extent practicable directly from the individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. 5 U.S.C. §552a(e)(2).

1. Collect from the subject first when the information sought is "objective and unalterable." Dong v. Smithsonian, 943 F. Supp. 69 (D.D.C. 1996) (holding that concerns over Plaintiff's possible reaction to an "unpleasant rumor" does not excuse noncompliance with the Act), *rev'd on other grounds*, 125 F.3d 877 (D.C. Cir. 1997); Waters v. Thornburgh, 888 F.2d 870 (D.C. Cir. 1989) (finding that the issue of plaintiff's attendance at bar examination is inalterable and that agency violated Act by interviewing others first); Brune v. IRS, 861 F.2d 1284 (D.C. Cir. 1988) (holding as permissible the earlier interview of witnesses in an investigation involving potential "shake-down" of audited taxpayers).

2. Collect from third parties when:

a. Verifying information (security or employment);

b. Seeking opinion or evaluation;

c. Unable to contact subject;

d. Collecting is exceptionally difficult (unreasonable cost or delay); or,

e. Consent or subject asks for third party collection.

f. *See, e.g.*, OMB Guidelines, 40 Fed. Reg. 28,948, 28,961 ("Practical considerations . . . may dictate that a third party source . . . be used as a source of information in some cases . . . It may well be that the kind of information needed can only be obtained from a third party").

C. Maintain no records regarding how an individual exercises First Amendment rights. 5 U.S.C. § 552a(e)(7).

1. Threshold. The record at issue must implicate the individual's First Amendment rights. *See* Cloud v. Heckler, 3 Gov't Disclosure Serv. (P-H) para 83,230, at 83,962 (W.D. Ark. Apr. 21, 1983) (filing of employee's letters criticizing agency, written while on duty, does not violate subsection (e)(7) because "[p]oor judgment is not protected by the First Amendment").

2. Exceptions.

a. Consent of the subject.

b. Authorized by statute. Hass v. United States Air Force, 848 F. Supp. 926 (D. Kan. 1994) (retaining copy of plaintiff's earlier FOIA requests is not the maintenance of information related to plaintiff's exercise of her First Amendment rights).

c. Pertinent to and within the scope of an authorized law enforcement activity. *Compare* Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982) (NSA's collection of international telegraphic communications and transfer or that data to the FBI properly within law enforcement exception of the Act, because FBI had reasonable cause to believe that Jabara was a foreign agent when it requested the summaries) *with* Clarkson v. IRS, 678 F.2d 1368 (11th Cir. 1982) (collection of appellant's political speeches in an IRS file labeled "Tax Protestors" constitutes violation of the Act).

3. Applies to all records, regardless of where maintained. Boyd v. Secretary of the Navy, 709 F.2d 684 (11th Cir. 1983) (holding that PA prohibition regarding collecting First Amendment information applied even when record not maintained in a system of records); Albright v. United States, 631 F. 2d 915 (D.C. Cir. 1980) ("desk drawer" storage of video of federal employees during a meeting explaining a denial of promotions held to be a record related to exercise of First Amendment rights).

D. Inform individuals asked to supply information of the authority for solicitation of the information and whether disclosure is mandatory or voluntary; the purpose for which the information is to be used; the routine uses applicable to the information; and the effects of not providing the information. This notice is general called a "**Privacy Act Advisement**." 5 U.S.C. § 552a(e)(3).

1. When required.

a. Notice **must** be provided when agency collects from an individual any personal information which will be kept in a system of records.

b. Notice **should** be given to third party sources of information at the time of collection. *See* Gardner v. United States, No. 96-1467, 1999 U.S. Dist. LEXIS 2195 (D.D.C. Jan. 29, 1999) (noting that although Act mandates actual notice of routine uses, "information in the instant case was not gathered from Plaintiff, but from third-parties"). *But see* Saunders v. Schweiker, 508 F. Supp. 305 (W.D.N.Y. 1981) (plain language of Act "does not in any way distinguish between first-party and third-party contacts").

2. Content of the Privacy Act Advisement:

a. The authority for collection;

b. The principal purpose for collection;

c. Whether disclosure is voluntary or mandatory;

d. The effect of not providing information; and,

e. The routine uses which may be made of the information. *See* Covert v. Harrington, 876 F.2d 751 (9th Cir. 1989) (Dep't of Energy disclosure of employee security forms to the Dep't of Justice improper because agency failed to notify its employees that the information in the files would be used for law enforcement purposes).

3. Location. "Placement of the Privacy Act advisory statement in a form should be in the following order of preference:

a. Below the title of the form and positioned so the individual will be advised of the requested information,

b. Within the body of the form with a notation of its location below the title of the form,

c. On the reverse of the form with a notation of its location below the title of the form,

d. Attached to the form as a tear-off sheet, or

e. Issued as a separate supplement to the form." *See* Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 18.

E. Accuracy requirements.

1. Maintain records used to make determinations about an individual with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness in the determination. 5 U.S.C. § 552a(e)(5). Perfect records are not required; reasonableness is the standard. Doe v. United States, 821 F.2d 694 (D.C. Cir. 1987) (*en banc*) (not inaccurate for agency to file ROI containing sharply conflicting accounts of unwitnessed interview between Dep't of State security agent and Doe, despite language that "there is no reason to doubt the statements made by [the] agent," since file also contains Doe's rebuttal); Edison v. Dep't of the Army, 672 F.2d 840 (11th Cir. 1982) (finding that appellant failed to show any causal connection between his incorrect ORB and the decision to pass him over for promotion, finding that there were many other possible factors which may have gone into the board's decision).

2. Before disseminating the record to a person other than an agency, unless disseminated pursuant to FOIA, the agency will make reasonable efforts to ensure the records are accurate, complete, timely and relevant for agency purposes. 5 U.S.C. § 552a(e)(6). *See* Pontecorvo v. FBI, No. 00-1511, slip op. at 20 (D.D.C. Sept. 30, 2001) (finding that "if the information gathered and contained within an individual's background records is the subjective opinion of witnesses, it is incapable of being verified as false and cannot constitute inaccurate statements under the Privacy Act").

F. Accounting for disclosures. "Each agency, with respect to each system of records under its control, must keep a record of the date, nature, and purpose of each disclosure of a record to any person or to another agency under subsection (b) and the name and address of the person or agency to whom the disclosure is made."

1. Disclosure accounting is required unless the record is disclosed within the agency (Exception 1) or pursuant to FOIA (Exception 2). 5 U.S.C. § 552a(c)(1).

2. Accounting of disclosures must be kept for five years or the life of the record, whichever is longer. *See* 5 U.S.C. § 552a(c)(2).

3. Except for disclosures made to law enforcement agencies, an individual is entitled, upon request, to access to accounting. *See* 5 U.S.C. § 552a(c)(3).

4. Agency must inform any person or other agency about any correction or notation of dispute made by the agency in accordance with a subject's amendment rights. *See* 5 U.S.C. § 552a(c)(4).

5. DA Form 4410-R may be used to record disclosure for accounting purposes.

G. Agency must make reasonable efforts to notify an individual when any record is made available to any person under compulsory process when such process becomes a matter of public record. 5 U.S.C. § 552a(e)(8). See Moore v. United States Postal Serv., 609 F. Supp. 681 (E.D.N.Y. 1985) ("§552a(e)(8) does not speak of advance notice of release").

H. Establish rules of conduct for persons dealing with Privacy Act records and instruct each person regarding the Act's requirements. 5 U.S.C. § 552a(e)(9).

I. Establish safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. 5 U.S.C. § 552a(e)(10).

VI. DISCLOSURE OF INFORMATION FROM SYSTEMS OF RECORDS

A. Disclosure prohibited. The "no disclosure without consent" rule: "No agency shall disclose any record . . . by any means of communication to any person, or to another agency, except pursuant to a written request by or with the prior written consent of the individual to whom the records pertains, unless an exception applies." 5 U.S.C. 5 U.S.C. § 552a(b).

1. Consent must be express. *See* Wiley v. Veterans Admin., 176 F.Supp 2d 747 (E.D. Mi. 2001) (prospective employees broadly worded "release," executed concurrent with employment application in 1990, served as valid consent for purpose of disclosure to employer in 1999).

2. "Disclosures" can be made by written, oral, electronic, or mechanical means. *See* OMB Guidelines, 40 Fed. Reg. 28948, 28953 (1975).

3. Prohibition applies only if disclosure is from a system of records.

a. Pertains to information initially retrieved from a system of records. Boyd v. Secretary of the Navy, 709 F.2d 684 (11th Cir. 1983) (memorandum documenting meeting between appellant and Navy supervisors not a record because it was not maintained by appellee in a group of records keyed to appellant's name); Henke v. Dep't of Commerce, 83 F.3d 1453 (D.C. Cir. 1996) (computer database was not a system of records as there is no evidence that agency regularly or even frequently used the names of the contact persons to obtain information about those persons).

b. Excludes knowledge independently derived. An employee's personal opinion or information drawn from personal memory is not equivalent to retrieval from a system of records. Kline v. HHS, 927 F.2d 522 (10th Cir. 1983) (holding that verbal information about employee derived from independent knowledge and not from an agency system of records are not subject to the Privacy Act). *But see* Bartel v. FAA, 725 F.2d 1403 (D.C. Cir. 1984) (holding "independent knowledge defense" is not available to employees personally involved in creation of record).

4. A later release of information previously known does not violate the Privacy Act. Hollis v. Department of the Army, 856 F.2d 1541 (D.C. Cir. 1988) (holding that when a release of service member's child care allotments consisted "merely of information . . . which the recipient of the release already knew, the Privacy Act is not violated"); FDIC v. Dye, 642 F.2d 833 (5th Cir. 1981). *But see* Pilon v. Department of Justice, 73 F.3d 1111 (D.C. Cir. 1996) (holding that Act violated by faxing document to a former employee previously familiar with the document's contents).

5. Privacy Act is not limited to extra-judicial disclosures; it applies even where a disclosure to a court during the course of litigation is undertaken. *See* Laningham v. Navy, 813 F.2d 1236 (D.C. Cir. 1987) (*per curium*) (holding that Navy did not intentionally and willfully disclose disability board information in civil trial in violation of PA). If while in litigation, an agency receives a request for Privacy Act information, counsel must object on the ground that the Privacy Act prohibits disclosure, or obtain a court order, *see* Exception 11 *infra*, permitting such disclosure.

B. There are **12 Exceptions** to the "no disclosure without consent" rule that permit third-party access to information without prior written consent of the subject of the record. 5 U.S.C. § 552a(b)(1)-(12).

1. **Exception 1**. The "Need to Know" exception. Disclosure to "officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1).

a. This exception authorizes intra-agency disclosures only for necessary, official purposes. *See* OMB Guidelines, 40 Fed. Reg. 28948, 28950-01, 28954 (1975).

(1) Improper uses are impermissible. *See* Parks v. IRS, 618 F.2d 677 (10th Cir. 1980) (disclosure of names of employees who did not purchase savings bonds, "for solicitation purposes," held improper); Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 37.

(2) Examples of proper "need to know" disclosures. Bigelow v. DOD, 217 F.3d 875 (D.C. Cir. 2000) (approving supervisor's review of appellant's personnel file related to supervisor's "continuing duty to make sure that [plaintiff] was worthy of trust"; supervisor "had a need to examine the file in view of the doubts that had been raised in his mind about [plaintiff] and [plaintiff's] access to the country's top secrets"); Britt v. Naval Investigative Serv., 886 F.2d 544 (3d Cir. 1989) (proper to disclosure investigative report to commander "since the Reserves might need to reevaluate Britt's access to sensitive information or the level of responsibility he was accorded"); Jones v. Dep't of the Air Force, 947 F. Supp. 1507 (D. Colo. 1996) (no violation for Air Force investigator to review medical and mental health records and then comment on the contents in ROI compiled in preparation for plaintiff's court-martial,

which was distributed to certain Air Force personnel); Hass v. United States Air Force, 848 F. Supp. 926, 932 (D. Kan. 1994) (upholding disclosure of mental health evaluation to officers who ultimately made decision to revoke plaintiff's security clearance and discharge her).

b. Are contractors who operate a system of records to accomplish an agency mission considered agency employees? Two cases have held yes. *See* Coakley v. Dep't of Transportation, 1994 U.S. Dist. LEXIS 21402 (D.D.C. Apr. 7, 1994); Hulett v. Dep't of the Navy, No. TH 85-310-C, slip op. (S.D. Ind. Oct. 26, 1987) (medical and personnel records disclosed to contractor/psychiatrist for purpose of assisting him in performing "fitness for duty" examination), ***aff'd***, 866 F.2d 432 (7th Cir. 1988) (unpublished table decision). *See also* Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 16. *But see* Taylor v. Orr, 1983 U.S. Dist. LEXIS 20334 (D.D.C. Dec. 5, 1983) (Sec'y of the Air Force violated the Act by providing plaintiff's examining physician a copy of her personnel records without her consent prior to a fitness-for-duty examination ordered by the secretary). OMB recommends use of a routine use to accomplish disclosures to contractors.

2. **Exception 2**. Disclosure **required** by the FOIA. 5 U.S.C. § 552a(b)(2). *See* Greentree v. United States Customs Serv., 674 F.2d 74, 79 (D.C. Cir. 1982) (subsection (b)(2) "represents a Congressional mandate that the Privacy Act not be used as a barrier to FOIA access").

a. The Privacy Act/FOIA interface typically involves FOIA Exemption 6, Protection of Personal Privacy, and FOIA Exemption 7(C), Records or Information Compiled for Law Enforcement Purpose the disclosure of which could reasonably be expected to result in an unwarranted invasion of privacy. Both exemptions require a balancing of the competing interests: Public Interests in Disclosure v. Invasion of Privacy. *See* Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

b. No discretionary release.

(1) No agency "discretionary disclosure" of information that is exempt under FOIA **and** subject to the Privacy Act. DOD v. FLRA, 510 U.S. 487 (1994).

(2) Agency must have an actual FOIA request to rely on exception 2. *See* Zeller v. United States, 467 F. Supp. 487, 503 (E.D.N.Y. 1979) (FOIA exception to Privacy Act does not apply because "nothing in the FOIA appears to require such information to be released in the absence of a request therefore"). *See also* OMB Memorandum for the Senior Agency Officials for Information Resources Management, SUBJECT: Privacy Act Guidance - Update, dated 24 May 1985. *Compare* Bartel v. FAA, 725 F.2d 1403 (D.C. Cir. 1984) (FOIA was meant to limit agency discretion to deny public access to information in its files, therefore,

the Privacy Act must be read generally to preclude nonconsensual disclosure of Privacy Act material unless the agency acts pursuant to a FOIA request) *with* Cochran v. United States, 770 F.2d 949 (11th Cir. 1985) (absence of written FOIA request irrelevant because overwhelming balance favored the public's right to disclosure of the information which related to a violation of the public trust by a senior government official; requested records would not be subject to withholding under any FOIA exemption).

c. Applying both statutes to requests for Privacy Act covered records. Analysis of third-party requests: Does a FOIA exemption permit withholding? If the answer is "Yes," (e.g., the Exemption 6 balancing test favors the subject's personal privacy), the record must be withheld. If the answer is "No," (e.g., the Exemption 6 balancing test favors the public interest), the record must be released.

3. **Exception 3**. Disclosure pursuant to published routine use. 5 U.S.C. § 552a(b)(3). Because it is potentially so broad, this is a controversial exception.

a. Threshold. The terms of this exception establish two requirements.

(1) First, the agency must provide constructive notice of the routine use through publication in the Federal Register.

(2) Second, the routine use must meet the compatibility requirement; that is, disclosure of record must be for a purpose that is compatible with the reason for which it was collected. 5 U.S.C. § 552a(a)(7). *See* Britt v. Naval Investigative Service, 886 F.2d 544 (3rd Cir. 1989) (holding that transfer of Marine Reservist's military criminal investigation file to his civilian federal employer did not meet the Act's compatibility requirement); Swenson v. United States Postal Service, 890 F.2d 1075 (9th Cir. 1989).

b. There are two types of routine uses: specific and general.

(1) Specific routine uses are strictly construed to cover only those uses listed within published systems notices. *See* Pontecorvo v. FBI, No. 00-1511, slip op. at 13-15 (D.D.C. Sept. 30, 2001) (ordering discovery to determine whether the agency "overstepped [the] explicit restrictions" contained in its routine use).

(a) Each service's list of systems notices can be found at: http://www.defenselink.mil/privacy/notices/

(b) An agency's construction of its routine use is entitled to deference. *See* Dep't of the Air Force, Scott Air Force Base, Ill. v. FLRA, 104 F.3d 1396, 1402 (D.C. Cir. 1997).

(2) General routine uses cover all of the agency's systems notices and provide broad disclosure guidance that may be interpreted to cover a range of activities, such as:

(a) To law enforcement agencies when record indicates a violation or potential violation of law.

(b) To other federal agencies on request for hiring, retention, security clearance, or licensing decisions by those agencies.

(c) In response to Congressional inquiries and private relief legislation. Pellerin v. VA, 790 F.2d 1553 (11th Cir. 1986). *But see* Swenson v. United States Postal Service, 890 F.2d 1075 (9th Cir. 1989) (disclosure beyond scope of inquiry).

(d) As required by international agreement.

(e) To the Department of Justice for litigation.

(f) For counter-intelligence purposes or enforcing laws which protect the national security.

4. **Exception 4**. Disclosure to the Bureau of Census. 5 U.S.C. § 552a(b)(4).

5. **Exception 5**. Disclosure for statistical research. 5 U.S.C. § 552a(b)(5).

6. **Exception 6**. Disclosure to the National Archives and Records Administration as a record having sufficient historical or other value to warrant its continued preservation, or for evaluation by the Archivist to determine whether the record has such value. 5 U.S.C. § 552a(b)(6).

7. **Exception 7**. Disclosure "to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought. 5 U.S.C. § 552a(b)(7). *See* Doe v. Naval Air Station, 768 F.2d 1229 (11th Cir. 1985) (oral request from detective insufficient).

8. **Exception 8**. Disclosure "to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual." 5 U.S.C. § 552a(b)(8).

a. Case law emphasizes emergency nature of exception.

b. Disclosure notification must be sent to last known address.

c. Individual about whom records are disclosed need not necessarily be the individual whose health or safety is at peril; *e.g.,* release of records on several individuals in order to identify an individual who was injured in an accident. *See* OMB's Privacy Act Guidelines, 40 Fed. Reg. 28,955 (1975); DePlanche v. Califano, 549 F. Supp. 685 (W.D. Mich. 1982).

9. **Exception 9**. Disclosure "to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee." 5 U.S.C. § 552a(b)(9).

a. Disclosure need not be based upon Congressional request. Devine v. United States, 202 F.3d 547 (2d Cir. 2000).

b. Disclosure must be to Congressional body, rather than member. Swenson v. U.S. Postal Service, 890 F.2d 1075 (9th Cir. 1989).

10. **Exception 10**. Disclosure to the Comptroller General in the course of the performance of the duties of the General Accounting Office. 5 U.S.C. § 552a(b)(10).

11. **Exception 11**. Disclosure "pursuant to the order of a court of competent jurisdiction." 5 U.S.C. § 552a(b)(11).

a. Excludes grand jury subpoenas. Doe v. DiGenova, 779 F.2d 74 (D.C. Cir. 1985).

b. Unclear whether exception covers orders from states courts, though there are no court cases on point and OMB has not issued formal guidance.

12. **Exception 12**. Disclosure to a consumer reporting agency in accordance with the Debt Collection Act. 5 U.S.C. § 552a(b)(12).

VII. ACCESS TO AND AMENDMENT OF RECORDS

A. Each agency that maintains a system of records **shal**l:

1. Access: "upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him . . . to review the record and have a copy made . . . ." 5 U.S.C. § 552a (d)(1); subject to ten exemptions discussed below.

2. Amendment: "permit the individual to request amendment of a record pertaining to him . . ." 5 U.S.C. § 552a(d)(2).

B. Access Issues.

1. Third party information in the subject/requester's file.

a. Remember the definition of a "record." If the information identifies requestor and pertains to requestor, the agency should release/permit access.

b. If the information does not identify the requestor or is not "about" the requestor, the agency may deny access. *See* Voelker v. IRS, 646 F.2d 332 (8th Cir. 1981); *compare* DePlanche v. Califano, 549 F. Supp 685 (W.D. Mich. 1982).

2. Medical records of minors. DOD Reg. 5400.11-R, para. C3.1.6.5.

a. The Privacy Act applies to "[citizens] of the United States or [aliens] lawfully admitted for permanent residence." Minors are protected by the Act because minority is not a disqualifier. 5 U.S.C. § 552a(a)(2), *see also* Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 9.

b. The Privacy Act provides that "the parent of any minor…may act on behalf of the individual." 5 U.S.C. § 552a(h).

c. Stateside.

(1) Definition of minor? State law.

(2) If a minor, may release records to parents unless prohibited by state law.

(3) Look to the law of the state in which the records are located as state laws differ on the issue of access to a minor's medical records based, in part, on the subject matter of the record (e.g., psychiatric records, treatment records for drug and alcohol abuse, sexual hygiene/reproductive records).

d. Overseas.

(1) Definition of minor? The Department of Defense deems the age of majority to be 18 years.

(2) Parental access. Parents have a general right of access to medical records of minors.

(3) Parents may be denied access only if **all** of the following four conditions are met:

(a) Minor was between ages 15 and 17 at the time of treatment.

(b) Treatment sought in program that promised to keep treatment records confidential.

(c) Minor specifically requested confidentiality.

(d) Parent did not have the minor's written authorization or a court order.

3. Access denied under Privacy Act, but accessible under FOIA.

a. The Privacy Act is not a FOIA Exemption 3 withholding statute. Provenzano v. DOJ, 717 F.2d 799 (3d Cir. 1983), *vacated as moot*, 469 U.S. 14 (1984).

b. Congress clarified the Privacy Act's status in the CIA Information Act, Pub. L. No. 98-477, § 2(c), 98 Stat. 2211, 2212 (1984) (codified at 5 U.S.C. § 552a(t)(2)).

C. Amendment Issues.

1. A subject may seek correction of facts but has no authority to demand the amendment of an agency employee's opinion or judgment.

a. Corrections are limited to facts, not judgments, under the Act. Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 4; Hewitt v. Grabicki, 794 F.2d 1373 (9th Cir. 1986).

b. A requestor may seek the amendment of agency judgments only if all underlying facts are discredited. Mueller v. Winter, 485 F.3d 1191 (D.C. Cir. 2007); RR v. Dep't of Army, 482 F. Supp. 770 (D.D.C. 1980) (*dictum*).

2. A subject may not use the Privacy Act to collaterally attack an agency decision, if that issue was already the subject of judicial or quasi-judicial action. Sugrue v. Derwinski, 26 F. 3d 8 (2d Cir. 1994).

a. Issues for which adequate judicial review is available. Henderson v. Social Security Administration, 908 F.2d 559 (10th Cir. 1990).

b. A subject must exhaust administrative remedies before filing suit for an agency's refusal to permit amendment. Cargill v. Marsh, 902 F.2d 1006 (D.C. Cir. 1990).

3. If, after an appeal, the agency refuses to amend the record, the agency must permit the individual to file a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and must notify the individual of the provisions for judicial review of the agency's action. 5 U.S.C. § 552a(d)(3).

4. In any subsequent disclosure of information about an individual who has filed a statement of disagreement, the agency must clearly note the portion of the record which is disputed and provide copies of the statement, and, if the agency deems it appropriate, a concise statement of the reasons for the agency's refusal to amend the record. 5 U.S.C. § 552a(d)(4).

a. Individual agency determines what "concise" means, but should be lenient.

b. Statements of disagreements often prove damaging to the requestor.

5. Where the agency has made prior disclosures of a disputed record and an accounting was made, the agency must inform prior recipients of any correction or notation of dispute that concerns the disclosed record. 5 U.S.C. § 552a(c)(4). *See* "Accounting for Disclosures," at para V.F, *supra*.

D. Burdens of Proof.

1. Access. 5 U.S.C. § 552a(g)(3)(A). Burden of proof is upon agency. Courts have authority to conduct a *de novo* review.

2. Amendment. 5 U.S.C. § 552a(d)(2)(B)(i). Burden of proof is upon the plaintiff to prove that record is not accurate, relevant, timely or complete. Mervin v. FTC, 591 F.2d 821 (D.C. Cir. 1978).

E. Processing an Access or Amendment Request.

1. Time Limits.

a. Access. The agency has 10 working days to acknowledge the request and must release/provide access within 30 working days.

b. Amendment.

(1) Amendment Guidelines.

(a) Army: "Periodic review and amendment of records" AR 25-22, para 8-1.

(b) Air Force: "Amending a Privacy Act Record." AFI 33-332, para 2.8.

(c) Custodian/System Manager has 10 working days to acknowledge request and 20 additional working days (30 total working days) to provide a final response. 5 U.S.C. § 552a(d); " Time Limits" DoD 5400.11-R, para. C3.3.7.

2. Appeal.

a. The requestor must appeal the agency action within 60 calendar days.

b. The Review Authority will decide the requestor's appeal within 30 working days, unless for "good cause" the head of the agency extends the decision for 30 more days. 5 U.S.C. § 552a(d)(3); DoD 5400.11-R, para. C3.3.7..

F. There are **ten exemptions** that deny access and amendment rights to the subject of a Privacy Act record. 5 U.S.C. § 552A (j) and (k).

1. Agencies may claim exemptions to deny a subject access to his own records.

a. Exemptions are not generally automatic; agency head must have previously published a regulation explaining why the exemption (other than (d)(5)) is applicable to that particular system.

b. Agencies are not entitled to improperly claimed exemptions. Ryan v. Dep't of Justice, 595 F.2d 954 (4th Cir. 1979).

c. Exemptions are strictly construed. Agencies have the burden of proof to deny a subject access to his or her own file.

2. One Special Exemption. 5 U.S.C. § 552a(d)(5).

a. "Nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding."

b. This is the only self-executing exemption.

c. Applies to administrative proceedings. Martin v. Office of Special Counsel, 819 F.2d 1181 (D.C. Cir. 1987); Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 27.

3. Two General Exemptions. 5 U.S.C. § 552a(j)(1)-(2).

a. The general exemptions cover records:

(1) Maintained by the CIA (5 U.S.C. § 552a (j)(1)); or,

(2) Maintained by an agency/component thereof which performs as its principal function any activity pertaining to law enforcement (5 U.S.C. § 552a (j)(2)).

b. According to the Defense Privacy Board, the exemption does not follow a record transferred from an exempt system to a nonexempt system. Defense Privacy Board Advisory Opinions Transmittal Memorandum 92-1, No. 31. *But see* Doe v. FBI, 936 F.2d 1346 (D.C. Cir. 1991).

c. There is no temporal limitation to these exemptions.

4. Seven Specific Exemptions. 5 U.S.C. § 552a(k)(1)-(7).

a. The special exemptions cover records that are:

(1) Classified (simply incorporates FOIA exemption 1 protections in the Privacy Act context). 5 U.S.C. § 552a(k)(1).

(2) Investigatory material compiled for law enforcement purposes not covered by 5 U.S.C. § 552a(j)(2) [the second general exemption]. 5 U.S.C. § 552a(k)(2).

(a) This exemption protects all information in the system of records unless the subject has been deprived of a federal right, privilege, or benefit as a result of the maintenance of the records.

(b) If so, the subject would be entitled to access to all material except that which would identify a confidential source who provided information under an express promise of confidentiality.

(3) Maintained in connection with providing protective services to the President of the United States or other individuals. 5 U.S.C. § 552a(k)(3).

(4) Required by statute to be maintained and used solely as statistical records. 5 U.S.C. § 552a(k)(4).

(5) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified material. 5 U.S.C. § 552a(k)(5).

(a) This is a narrow exemption which is limited to the protection of a confidential source who provided the information pursuant to an **express** promise of confidentiality.

(b) Applicable even though the source of the confidential information is known to the requester. Volz v. Dep't of Justice, 619 F.2d 49 (10th Cir. 1980).

(c) There is no temporal limit to the protection.

(d) Also includes material compiled to determine whether a federal grant will be awarded. Henke v. United States Dep't of Commerce, 83 F.3d 1445 (D.C. Cir. 1996).

(6) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process. 5 U.S.C. § 552a(k)(6).

(a) Release of material that implicates the applicant evaluation system "would give future applicants an unfair advantage and would impair the usefulness and value of the system." Patton v. Federal Bureau of Investigations, 626 F. Supp. 445 (M.D. Pa. 1985).

(b) Robinett v. U.S. Postal Service, Civil Action No.: 02-1094, 2002 U.S. Dist. LEXIS 13779 (E.D. La. Jul. 24, 2002) (scoring evaluation information on employment application fell within the parameters of an exemption statute under the FOIA and 5 U.S.C. § 552a(k)(6) of the Privacy Act).

(7) Evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a confidential source who was granted an express promise of confidentiality. 5 U.S.C. § 552a(k)(7). *See also,* May v. Dep't of Air Force, 777 F.2d 1012 (5th Cir. 1985).

5. Summary: Analysis of first person access requests:

a. Does a Privacy Act exemption apply (e.g., the document is a law enforcement record or prepared in anticipation of litigation)? If the answer is "No," the agency must grant access to the document. If the answer is "Yes," the agency may withhold.

b. Does a FOIA exemption apply (e.g., on-going LEA investigation under 7(C))? If the answer is "Yes," the agency may withhold the document. If the answer is "No," the agency must release.

c. An agency may only withhold a record from a subject ONLY when Exemptions apply under both the FOIA and Privacy Act.

VIII. CRIMINAL PENALTIES.

A. "Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than **$5,000**." 5 U.S.C. § 552a(i). *See, e.g*., United States v. Trabert, 978 F.Supp 1368 (D.Colo. 1997)

B. "Any officer or employee of an agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(2).

C. "Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(3).

D. Criminal action is against the individual, not the agency.

IX. CIVIL REMEDIES.

A. Statutory. 5 U.S.C. § 552a(g)(1).

1. Violations and remedies.

a. Wrongful refusal to amend. 5 U.S.C. § 552a(g)(1)(A); 5 U.S.C. § 552a(g)(2)(A)-(B). Remedy: Enjoin/order amendment; attorney fees/costs.

b. Wrongful denial of access. 5 U.S.C. § 552a(g)(1)(B); 5 U.S.C. § 552a(g)(3)(A). Remedy: Enjoin from withholding; provide in camera inspection; attorney fees/costs.

c. Failure to maintain accurate, timely, complete, and relevant records resulting in an adverse determination. 5 U.S.C. § 552a(g)(1)(C); 5 U.S.C. § 552a(g)(4)(A)-(B). Remedy: If agency acted in an intentional/willful manner, U.S. is liable for: Actual damages but not less than $1,000; attorney fees/costs.

d. Failure to comply with another provision causing an adverse effect. 5 U.S.C. § 552a(g)(1)(D); 5 U.S.C. § 552a(g)(4)(A)-(B). Remedy: If agency acted in an intentional/willful manner, U.S. liable for: Actual damages but not less than $1,000; attorney fees/costs.

2. Civil remedies are solely against the agency.

3. Courts are not free to create remedies greater than those granted by the statute. Edison v. Dep't of Army, 672 F.2d 840 (11th Cir. 1982).

4. Intentional or willful refers to the intentional or willful failure to abide by the Act. Andrews v. VA, 838 F.2d 418 (10th Cir. 1988); Tijerina v. Walters, 821 F.2d 789 (D.C. Cir. 1987); Albright v. U.S., 732 F.2d 181 (D.C. Cir. 1984).

5. Privacy Act does not mandate agency to create and maintain files, and destruction of an official record does not give right to a Privacy Act cause of action. Tufts v. Dep't of Air Force, 793 F.2d 259 (10th Cir. 1986).

6. Damages.

a. Doe v. Chao, 540 U.S. 614 (2004) (ruling that "actual damages" must be proved to recover the statutory minimum of $1,000 or damages beyond the minimum; out-of-pocket damages will suffice but it is not clear if solely nonpecuniary damages for mental injuries are sufficient). *See also* Jacobs v. Nat'l Drug Intelligence Ctr, 548 F. 3d 375 (5th Cir. 2008) (upholding $100,000 award for emotional distress, noting that Doe v. Chao did not authoritatively rule on this issue).

b. Cummings v. Dep't of the Navy, 279 F. 3d 1051 (D.C. Cir. 2002) (holding Feres v. United States, 340 U.S. 135 (1950), inapplicable to Service members Privacy Act lawsuit, whether seeking injunctive relief or damages).

7. Attorney's Fees. The Privacy Act includes "fee shifting" provisions. Anderson v. Dep't of Treasury, 648 F.2d 1 (D.C. Cir. 1979).

a. Threshold requirement: plaintiff must substantially prevail. Sweatt v. U.S. Navy, 683 F.2d 420 (D.C. Cir. 1982).

b. Not paid to a *pro se* litigant even if plaintiff is an attorney. Manos v. Department of the Air Force, 829 F. Supp. 1191 (N.D. Cal. 1993).

c. Only permitted for litigation; not administrative actions. Kennedy v. Andrus, 459 F. Supp. 240 (D.D.C. 1978), *aff'd,* 612 F. 2d 586 (D.C. Cir. 1980)(table cite).

8. Two-year statute of limitations governs Privacy Act actions. 5 U.S.C. § 552a(g)(5). Bowyer v. Department of Air Force, 875 F.2d 632 (7th Cir. 1989); Tijerina v. Walters, 821 F.2d 789 (D.C. Cir. 1987).

B. Tort Actions.

1. One court has held that the Privacy Act "does not limit the remedial rights of persons to pursue whatever remedies they may have under the [Federal Tort Claims Act] for privacy violations consisting of record disclosures." O'Donnell v. United States, 891 F. 2d 1079 (3d Cir. 1989).

2. It now appears settled that the Privacy Act consists of a "comprehensive legislative scheme" that precludes Bivens constitutional tort remedies. *See* Wilson v. Libby, 535 F. 3d 697 (D.C. Cir. 2008); Downie v. City of Middleburg Heights, 301 F. 3d 688 (6th Cir. 2002).

3. Note also that the statutory scheme established under "FOIA precludes the creation of a Bivens remedy." Johnson v. Executive Office for U.S. Attorneys, 310 F.3d 771 (D.C. Cir. 2002).

X. SOCIAL SECURITY NUMBERS.

A. Section 7(a)(1). (Enacted as part of the Privacy Act, but not codified.) "It shall be unlawful for any Federal, State, or local governmental agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." By its terms, Section 7 does not apply to:

1. Any disclosure required by Federal statute, or,

2. Any disclosure required under any Federal, State, or local statute or regulation in existence and operating before 1 January 1975 to verify the identity of the individual.

B. "Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." Section 7(b).

C. DOD Regulations

1. DOD 5400.11-R, Chapter 2, para C2.1.2. - Collecting Social Security Numbers.

2. Army Regulation 25-22, para 5-3.c. – "The current use of the Department of Defense ID (DOD ID) number is gradually replacing use of the SSN. Increased use of the DOD ID helps to minimize use of the SSN and assists with the safeguarding process."

3. SECNAVINST 5211.5F, para 5.c. – "Use of Social Security Numbers (SSN) will be reduced or eliminated wherever possible[.]"

4. AFI 33-332, para 5.3 – "When law, executive order, or regulation does not require disclosing the SSN or if the SOR was created after January 1, 1975, a SSN may be requested, but the individual is not required to disclose it. If the individual refuses to provide their information, use alternative means of identifying records."

D. DODI 1000.30, August 1, 2012 , incorporates and cancels (DTM) 2007-015-USD(P&R)—"DoD Social Security Number (SSN) Reduction Plan."

1. This instruction establishes the policy and assigns responsibility for reduction of SSN in DoD. It is the DoD policy to reduce or eliminate the use of SSNs wherever possible.

2. The use of the SSN includes the SSN in any form, including, but not limited to, truncated, masked, partially masked, encrypted or disguised. SSNs shall be used in approved form when they meet the criteria established in the instruction.

3. The identified acceptable uses include:
   a. Law Enforcement, National Security, Credentialing
   b. Security Clearance Investigation or Verification
   c. Interactions With Financial Institutions
   d. Confirmation of Employment Eligibility
   e. Administration of Federal Worker's Compensation
   f. Federal Taxpayer Identification Number
   g. Computer Matching
   h. Foreign Travel
   i. Geneva Conventions Serial Number
   j. Noncombatant Evacuation Operations
   k. Legacy System Interface
   l. Operational Necessity
   m. Other Cases (with specified documentation)

E. Section 7 applies to state and local agencies as well.

XI. CONCLUSION.

The underlying purpose of the Privacy Act is to give citizens more control over personal information collected by the Federal Government and how that information is used. The act accomplishes this in four basic ways. It seeks to establish sound information practices in the federal agencies and requires public notice of all systems of records. It

requires that the information contained in these record systems be accurate, complete, relevant, and timely. It provides procedures whereby individuals can inspect and correct inaccuracies in almost all Federal records about themselves. Finally, it limits disclosure of records; requires agencies to keep an accurate accounting of disclosures; and, with certain exceptions, makes these disclosures available to the subject of the record. In the event that the statute is violated there are both criminal sanctions and civil remedies.

CHAPTER C

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

45 CFR PARTS 160 AND 164, SUBPARTS A AND E

Note: This chapter is a compilation of HIPAA guidance from the U.S. Department of Health and Human Services, Defense Health Agency, and Military Health System.

January 2021

OCR PRIVACY BRIEF

SUMMARY OF THE HIPAA PRIVACY RULE

HIPAA Compliance Assistance

SUMMARY OF
THE HIPAA PRIVACY RULE

Contents

SUMMARY OF
THE HIPAA PRIVACY RULE

Introduction

The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). [1] The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to 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. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

This is a summary of key elements of the Privacy Rule and not a complete or comprehensive guide to compliance. Entities regulated by the Rule are obligated to comply with all of its applicable requirements and should not rely on this summary as a source of legal information or advice. To make it easier for entities to review the complete requirements of the Rule, provisions of the Rule referenced in this summary are cited in notes at the end of this document. To view the entire Rule, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa. In the event of a conflict between this summary and the Rule, the Rule governs.

Links to the OCR Guidance Document are provided throughout this paper. Provisions of the Rule referenced in this summary are cited in endnotes at the end of this document. To review the entire Rule itself, and for other additional helpful information about how it applies, see the OCR website: http://www.hhs.gov/ocr/hipaa.

Statutory & Regulatory Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the *Administrative Simplification* provisions.

HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within

	three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.[2] In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.[3] A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E on the OCR website: http://www.hhs.gov/ocr/hipaa.
Who is Covered by the Privacy Rule	The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). For help in determining whether you are covered, use the decision tool at: https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf. **Health Plans.** Individual and group plans that provide or pay the cost of medical care are covered entities.[4] Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center,[5] or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance. **Health Care Providers.** Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.[6] Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

	Health Care Clearinghouses. *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. [7] In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.[8] Health care clearinghouses include billing services, repricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.
Business Associates	**Business Associate Defined.** In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.[9] Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. A covered entity can be the business associate of another covered entity. **Business Associate Contract.** When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.[10] Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the Rule. Covered entities that have an existing written contract or agreement with business associates prior to October 15, 2002, which is not renewed or modified prior to April 14, 2003, are permitted to continue to operate under that contract until they renew the contract or April 14, 2004, whichever is first.[11] Sample business associate contract language is available on the OCR website at: http://www.hhs.gov/ocr/hipaa/contractprov.html. Also see OCR "Business Associate" Guidance.
What Information is Protected	**Protected Health Information.** The Privacy Rule protects 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. The Privacy Rule calls this information "*protected health information (PHI)*."[12]

	"Individually identifiable health information" is information, including demographic data, that relates to: • the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual, or • the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. **De-Identified Health Information.** There are no restrictions on the use or disclosure of de-identified health information.[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.[15]
General Principle for Uses and Disclosures	**Basic Principle.** A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.[16] **Required Disclosures.** A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.[17] See OCR "Government Access" Guidance.
Permitted Uses and Disclosures	**Permitted Uses and Disclosures.** A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and

(6) Limited Data Set for the purposes of research, public health or health care operations.[18] Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.[19] A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See OCR "Treatment, Payment, Health Care Operations" Guidance.

> ***Treatment*** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.[20]
>
> ***Payment*** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual[21] and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
>
> ***Health care operations*** are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.[22]

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.[23]

Obtaining "consent" (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities.[24] The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

> ***Facility Directories.*** It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility.[25] The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.
>
> ***For Notification and Other Purposes.*** A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care. [26] This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.[27] See OCR "Incidental Uses and Disclosures" Guidance.

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.[28] These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

> ***Required by Law.*** Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by

statute, regulation, or court orders).[29]

Public Health Activities. Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.[30] See OCR "Public Health" Guidance; CDC Public Health and HIPAA Guidance.

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[31]

Health Oversight Activities. Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.[32]

Judicial and Administrative Proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.[33]

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.[34]

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.[35]

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.[36]

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.[37] The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought.[38] A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).[39] See OCR "Research" Guidance; NIH Protecting PHI in Research.

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.[40]

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.[41]

	Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.[42] See OCR "Workers' Compensation" Guidance. **(6) Limited Data Set**. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.[43] A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.
Authorized Uses and Disclosures	**Authorization.** A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.[44] A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.[45] An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.[46] **Psychotherapy Notes[47].** A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions[48]: • The covered entity who originated the notes may use them for treatment. • A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law. **Marketing.** Marketing is any communication about a product or service that encourages recipients to purchase or use the product or service.[49] The Privacy Rule carves out the following health-related activities from this definition of marketing: • Communications to describe health-related products or services, or payment

	for them, provided by or included in a benefit plan of the covered entity making the communication; • Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefits plan; • Communications for treatment of the individual; and • Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual. Marketing also is an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity's provision of promotional gifts of nominal value. No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition. An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact. See OCR "Marketing" Guidance.
Limiting Uses and Disclosures to the Minimum Necessary	**Minimum Necessary.** A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.[50] A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. See OCR "Minimum Necessary" Guidance. The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules. **Access and Uses.** For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of

	protected health information to which access is needed, and any conditions under which they need the information to do their jobs. **Disclosures and Requests for Disclosures.** Covered entities must establish and implement policies and procedures (which may be standard protocols) for *routine, recurring disclosures, or requests for disclosures,* that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, covered entities must develop criteria designed to limit disclosures to the information reasonably necessary to accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria. **Reasonable Reliance.** If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.
Notice and Other Individual Rights	**Privacy Practices Notice.** Each covered entity, with certain exceptions, must provide a notice of its privacy practices.[51] The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans. See OCR "Notice" Guidance. • **Notice Distribution.** A covered health care provider with a *direct treatment relationship* with individuals must deliver a privacy practices notice to patients starting April 14, 2003 as follows: o Not later than the first service encounter by personal delivery (for patient visits), by automatic and contemporaneous electronic response (for electronic service delivery), and by prompt mailing (for telephonic service delivery); o By posting the notice at each service delivery site in a clear and prominent place where people seeking service may reasonably be expected to be able to read the notice; and o In emergency treatment situations, the provider must furnish its notice as soon as practicable after the emergency abates.

Covered entities, whether *direct treatment providers* or *indirect treatment providers* (such as laboratories) or *health plans* must supply notice to anyone on request.[52] A covered entity must also make its notice electronically available on any web site it maintains for customer service or benefits information.

The covered entities in an *organized health care arrangement* may use a joint privacy practices notice, as long as each agrees to abide by the notice content with respect to the protected health information created or received in connection with participation in the arrangement.[53] Distribution of a joint notice by any covered entity participating in the organized health care arrangement at the first point that an OHCA member has an obligation to provide notice satisfies the distribution obligation of the other participants in the organized health care arrangement.

A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment, and send a reminder to every enrollee at least once every three years that the notice is available upon request. A health plan satisfies its distribution obligation by furnishing the notice to the "named insured," that is, the subscriber for coverage that also applies to spouses and dependents.

- **Acknowledgement of Notice Receipt.** A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.[54] The Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement. The provider is relieved of the need to request acknowledgement in an emergency treatment situation.

Access. Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's *designated record set*.[55] The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.[56] The Rule excepts from the right of access the following protected health information: psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.[57] Covered entities may impose reasonable, cost-based fees for the cost of copying and postage.

Amendment. The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is

	inaccurate or incomplete.[58] If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.[59] If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity. **Disclosure Accounting.** Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.[60] The maximum disclosure accounting period is the six years immediately preceding the accounting request, except a covered entity is not obligated to account for any disclosure made before its Privacy Rule compliance date. The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures. Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities. **Restriction Request.** Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.[61] A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[62] **Confidential Communications Requirements.** Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.[63] For example, an individual may request that the provider communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card. Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment. Any covered entity may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

Administrative Requirements	HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources. **Privacy Policies and Procedures.** A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.[64] **Privacy Personnel.** A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.[65] **Workforce Training and Management.** Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).[66] A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions.[67] A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.[68] **Mitigation.** A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.[69] **Data Safeguards.** A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.[70] For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. See OCR "Incidental Uses and Disclosures" Guidance. **Complaints.** A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.[71] The covered entity must explain those procedures in its privacy practices notice.[72] Among other things, the covered entity must identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS. **Retaliation and Waiver.** A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.[73] A covered entity may not

	require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.[74] **Documentation and Record Retention.** A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.[75] **Fully-Insured Group Health Plan Exception.** The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.[76]
Organizational Options	The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections. **Hybrid Entity.** The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity."[77] (The activities that make a person or organization a covered entity are its "covered functions."[78]) To be a hybrid entity, the covered entity must designate in writing its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A covered entity that does not make this designation is subject in its entirety to the Privacy Rule. **Affiliated Covered Entity.** Legally separate covered entities that are affiliated by common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.[79] The designation must be in writing. An affiliated covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions. **Organized Health Care Arrangement.** The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as "organized health care arrangements."[80] Covered entities in an organized health care arrangement can share protected health information with each other for the arrangement's joint health care operations.[81] **Covered Entities With Multiple Covered Functions.** A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.[82] The covered entity may not use or disclose the protected health information of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function.

	Group Health Plan disclosures to Plan Sponsors. A group health plan and the health insurer or HMO offered by the plan may disclose the following protected health information to the "plan sponsor"—the employer, union, or other employee organization that sponsors and maintains the group health plan[83]: • Enrollment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan. • If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. "Summary health information" is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified protected health information). • Protected health information of the group health plan's enrollees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the protected health information. These restrictions must include the representation that the plan sponsor will not use or disclose the protected health information for any employment-related action or decision or in connection with any other benefit plan.
Other Provisions: Personal Representatives and Minors	**Personal Representatives.** The Privacy Rule requires a covered entity to treat a *"personal representative"* the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Rule.[84] A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual. **Special case: Minors.** In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to State and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment. See OCR "Personal Representatives" Guidance.

State Law	**Preemption.** In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.[85] "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.[86] The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits. **Exception Determination.** In addition, preemption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law: • Is necessary to prevent fraud and abuse related to the provision of or payment for health care, • Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation, • Is necessary for State reporting on health care delivery or costs, • Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or • Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.
Enforcement and Penalties for Noncompliance	**Compliance.** Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule.[87] The Rule provides processes for persons to file complaints with HHS, describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews. **Civil Money Penalties.** HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.[88] That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

	Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment.[89] The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.
Compliance Dates	**Compliance Schedule.** All covered entities, except "small health plans," must be compliant with the Privacy Rule by April 14, 2003.[90] Small health plans, however, have until April 14, 2004 to comply. **Small Health Plans.** A health plan with annual receipts of not more than $5 million is a small health plan.[91] Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts.[92] See What constitutes a small health plan?
Copies of the Rule & Related Materials	The entire Privacy Rule, as well as guidance and additional materials, may be found on our website, http://www.hhs.gov/ocr/hipaa.

End Notes

[1] Pub. L. 104-191.

[2] 65 FR 82462.

[3] 67 FR 53182.

[4] 45 C.F.R. §§ 160.102, 160.103.

[5] Even if an entity, such as a community health center, does not meet the definition of a health plan, it may, nonetheless, meet the definition of a health care provider, and, if it transmits health information in electronic form in connection with the transactions for which the Secretary of HHS has adopted standards under HIPAA, may still be a covered entity.

[6] 45 C.F.R. §§ 160.102, 160.103; *see* Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). The transaction standards are established by the HIPAA Transactions Rule at 45 C.F.R. Part 162.

[7] 45 C.F.R. § 160.103.

[8] 45 C.F.R. § 164.500(b).

[9] 45 C.F.R. § 160.103.

[10] 45 C.F.R. §§ 164.502(e), 164.504(e).

[11] 45 C.F.R. § 164.532

[12] 45 C.F.R. § 160.103.

[13] 45 C.F.R. § 160.103

[14] 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[15] The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the "safe harbor" method of de-identification: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses: (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and ® any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information. 45 C.F.R. § 164.514(b).

[16] 45 C.F.R. § 164.502(a).

[17] 45 C.F.R. § 164.502(a)(2).

[18] 45 C.F.R. § 164.502(a)(1).

[19] 45 C.F.R. § 164.506(c).

[20] 45 C.F.R. § 164.501.

[21] 45 C.F.R. § 164.501.

[22] 45 C.F.R. § 164.501.

[23] 45 C.F.R. § 164.508(a)(2)

[24] 45 C.F.R. § 164.506(b).

[25] 45 C.F.R. § 164.510(a).

[26] 45 C.F.R. § 164.510(b).

[27] 45 C.F.R. §§ 164.502(a)(1)(iii).

[28] *See* 45 C.F.R. § 164.512.

[29] 45 C.F.R. § 164.512(a).

[30] 45 C.F.R. § 164.512(b).

[31] 45 C.F.R. § 164.512(a), (c).

[32] 45 C.F.R. § 164.512(d).

[33] 45 C.F.R. § 164.512(e).

[34] 45 C.F.R. § 164.512(f).

[35] 45 C.F.R. § 164.512(g).

[36] 45 C.F.R. § 164.512(h).

[37] The Privacy Rule defines research as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." 45 C.F.R. § 164.501.

[38] 45 C.F.R. § 164.512(i).

[39] 45 CFR § 164.514(e).

[40] 45 C.F.R. § 164.512(j).

[41] 45 C.F.R. § 164.512(k).

[42] 45 C.F.R. § 164.512(l).

[43] 45 C.F.R. § 164.514(e). A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses: (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any comparable images. 45 C.F.R. § 164.514(e)(2).

[44] 45 C.F.R. § 164.508.

[45] A covered entity may condition the provision of health care solely to generate protected health information for disclosure to a third party on the individual giving authorization to disclose the

information to the third party. For example, a covered entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual's authorization to disclose the results of that examination to the life insurance issuer. A health plan may condition enrollment or benefits eligibility on the individual giving authorization, requested before the individual's enrollment, to obtain protected health information (other than psychotherapy notes) to determine the individual's eligibility or enrollment or for underwriting or risk rating. A covered health care provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual's protected health information for the research. 45 C.F.R. 508(b)(4).

[46] 45 CFR § 164.532.

[47] "Psychotherapy notes" means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R. § 164.501.

[48] 45 C.F.R. § 164.508(a)(2).

[49] 45 C.F.R. §§ 164.501 and 164.508(a)(3).

[50] 45 C.F.R. §§ 164.502(b) and 164.514 (d).

[51] 45 C.F.R. §§ 164.520(a) and (b). A group health plan, or a health insurer or HMO with respect to the group health plan, that intends to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, must state that fact in the notice. Special statements are also required in the notice if a covered entity intends to contact individuals about health-related benefits or services, treatment alternatives, or appointment reminders, or for the covered entity's own fundraising.

[52] 45 C.F.R. § 164.520(c).

[53] 45 C.F.R. § 164.520(d).

[54] 45 C.F.R. § 164.520(c).

[55] 45 C.F.R. § 164.524.

[56] 45 C.F.R. § 164.501.

[57] A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional (who is designated by the covered entity and who did not participate in the original decision to deny), when a licensed health care professional has determined, in the exercise of professional judgment, that: (a) the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (b) the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or (c) the request for access is made by the individual's personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting

to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. § 552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 C.F.R. § 164.524.

[58] 45 C.F.R. § 164.526.

[59] Covered entities may deny an individual's request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 164.526(a)(2).

[60] 45 C.F.R. § 164.528.

[61] 45 C.F.R. § 164.522(a).

[62] 45 C.F.R. § 164.522(a). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.

[63] 45 C.F.R. § 164.522(b).

[64] 45 C.F.R. § 164.530(i).

[65] 45 C.F.R. § 164.530(a).

[66] 45 C.F.R. §160.103.

[67] 45 C.F.R. § 164.530(b).

[68] 45 C.F.R. § 164.530(e).

[69] 45 C.F.R. § 164.530(f).

[70] 45 C.F.R. § 164.530(c).

[71] 45 C.F.R. § 164.530(d).

[72] 45 C.F.R. § 164.520(b)(1)(vi).

[73] 45 C.F.R. § 164.530(g).

[74] 45 C.F.R. § 164.530(h).

[75] 45 C.F.R. § 164.530(j).

[76] 45 C.F.R. § 164.530(k).

[77] 45 C.F.R. §§ 164.103, 164.105.

[78] 45 C.F.R. § 164.103.

[79] 45 C.F.R. §164.105. Common ownership exists if an entity possesses an ownership or equity interest of five percent or more in another entity; common control exists if an entity has the direct or indirect power significantly to influence or direct the actions or policies of another entity. 45 C.F.R. §§ 164.103.

[80] The Privacy Rule at 45 C.F.R. § 160.103 identifies five types of organized health care arrangements:

- A clinically-integrated setting where individuals typically receive health care from more than one provider.
- An organized system of health care in which the participating covered entities hold themselves out to the public as part of a joint arrangement and jointly engage in

utilization review, quality assessment and improvement activities, or risk-sharing payment activities.

- A group health plan and the health insurer or HMO that insures the plan's benefits, with respect to protected health information created or received by the insurer or HMO that relates to individuals who are or have been participants or beneficiaries of the group health plan.
- All group health plans maintained by the same plan sponsor.
- All group health plans maintained by the same plan sponsor and all health insurers and HMOs that insure the plans' benefits, with respect to protected health information created or received by the insurers or HMOs that relates to individuals who are or have been participants or beneficiaries in the group health plans.

[81] 45 C.F.R. § 164.506(c)(5).

[82] 45 C.F.R. § 164.504(g).

[83] 45 C.F.R. § 164.504(f).

[84] 45 C.F.R. § 164.502(g).

[85] 45 C.F.R. §160.203.

[86] 45 C.F.R. § 160.202.

[87] 45 C.F.R.§ 160.304

[88] Pub. L. 104-191; 42 U.S.C. §1320d-5.

[89] Pub. L. 104-191; 42 U.S.C. §1320d-6.

[90] 45 C.F.R. § 164.534.

[91] 45 C.F.R. § 160.103.

[92] Fully insured health plans should use the amount of total premiums that they paid for health insurance benefits during the plan's last full fiscal year. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine proxy measures to determine their total annual receipts.

Information Paper

The Federal Privacy Act of 1974 and HIPAA Privacy Rule of 1996: A Comparison

Introduction

While health care providers have a long tradition of safeguarding private health information, protection of patient rights has recently been at the forefront of discussion. The old system of storing private patient information in locked filing cabinets is no longer practical or feasible—modern technology now allows for the rapid transmission of medical information electronically. However, along with this ease of sharing come new concerns regarding the confidentiality and protection of patient information. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule of 1996 provides clear standards for protection of personal health information or Protected Health Information (PHI). Prior to the Privacy Rule, PHI could be distributed without notice or authorization by the patient for reasons other than the patient's medical treatment and/or health care payment. While improving the efficiency of the healthcare delivery system, the act protects the privacy of PHI by simplifying the processes involved in transmitting data by standardizing electronic data interchange. This act sought to close a gap in the 1974 Privacy Act, which provided some safeguards to the collection and use of personal information by the federal government and its entities.

The Privacy Act of 1974, Public Law 93-579

The Privacy Act of 1974 provides individuals the right of access to information concerning themselves that is maintained by any federal agency in the Executive Branch. The Act also established controls over what personal information the federal government collects and how it uses or discloses that information. The Act arose out of concerns about how the creation and use of computerized databases might impact individuals' privacy rights. It safeguards privacy with the use of four personal data rights: Government agencies must show an individual any records kept on him or her; Agencies must follow certain principles, called "fair information practices," regarding personal data. Agencies are restricted in how they can share individual data with other people and agencies; Individuals may sue the government for violating the Act's provisions.

Health Insurance Portability and Accountability Act of 1996

The HIPAA Privacy Rule *(45 CFR Parts 160 and 164)*

HIPAA improves the efficiency and effectiveness of the health care industry in three primary ways; 1) by administrative simplifications provisions that develop single and universal claims and payment transaction codes, 2) by protecting the privacy and security of PHI, and 3) by providing provisions for the enforcement of its rules. The scope of HIPAA encompasses the following entities: health care plans, health care clearinghouses, and all health care providers who conduct certain health care transactions electronically.

The Privacy Rule is the foundation for federal protection for the privacy of PHI. PHI includes individually identifiable health information related to the past, present or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Even the fact that an individual received medical care is protected information under the regulation.

Privacy Rights

Together, the 1996 HIPPA Privacy Rule and the 1974 Privacy Act allow patients more rights and control over personal and medical information. In combination the acts do the following:

- Set boundaries on the use and release of personal data;
- Generally limit release of information to the minimum reasonably needed for the purpose of the disclosure.
- Establish safeguard standards for protecting the privacy of personal data.
    - Enable individuals to learn how their data may be used and about certain disclosures of their data that have been made
    - Empower individuals to control certain uses and disclosures of their personal data.
- Generally give individuals the right to examine and obtain a copy of their own personal data and request corrections.
- Hold violators accountable, with civil and criminal penalties that can be imposed if they violate individuals' rights.

Oversight

The Privacy Act empowers the Director of the Office of Management and Budget to develop regulations and guidelines on how agencies should implement the Act.

HIPAA empowers Health and Human Services (HHS) Office for Civil Rights to enforce the Privacy Rule by promoting voluntary compliance and using civil monetary penalties.

Penalties for Violations of Privacy

Both acts impose penalties on violators. The HIPAA Privacy Rule is the stricter of the two, imposing both civil and criminal penalties for violations of privacy. Penalties are generally assessed when organizations or individuals act with willful neglect or intent to cause harm. Civil penalties are specified at $100 per violation, not to exceed $25,000 per person per year for identical violations. Criminal penalties for wrongful disclosure of PHI can go up to $250,000 and/or 10 years imprisonment if the offense is committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm.
The 1974 Privacy Act gives an individual the right to sue the federal government if it violates the statue. In addition:

- Any officer or employer of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information, and conveys that information to any person or agency not entitled to receive it shall be guilty of a misdemeanor and fined not more than $5,000.
- Any officer or employee of an agency who willfully maintains a system of records for personal use shall be guilty of a misdemeanor and fined not more that $5000.

Any person who knowingly and willfully requests or obtains and record concerning an individual from an agency under false pretense shall be guilty of a misdemeanor and fined not more than $5000.

Discussion

The purpose of both acts was to strengthen the rights of the public in regards to the collection and use private information. Both work together to achieve the goal of protecting the privacy of personal information. Though HIPAA focuses mainly on medical information, the HIPAA Privacy Rule provision strengthens the intent of the Privacy Right Act of 1974 in that it requires all Federal agencies and/or Federal contractors that maintain personal records of individuals to adhere to the Privacy Rule’s requirements and comply with the Privacy Act.

Comments

The Acts differ in that the 1974 Act covers overall personal data collection and use by the federal government, not private entities. HIPAA seeks to close this gap by targeting an industry that has more information on the public than the government—the medical field. HIPAA is more specific because it only targets medical information—but it is far reaching because it closes all of this personal data off to others, including the government, if they cannot show a compelling interest for having access to this data.

The Military Command Exception and Disclosing PHI of Armed Forces Personnel

Introduction

This paper provides guidance on the use and disclosure of Armed Forces personnel PHI by covered entities for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. This "Military Command Exception" permits the use and disclosure of PHI that would otherwise be prohibited by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

Definitions

Covered Entity: A health plan or a health care provider that transmits any health information in electronic form in connection with a HIPAA standard transaction.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a covered entity in its role as employer.

Use: With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Discussion

Under the Military Command Exception, a covered entity may disclose the PHI of Service members for authorized activities to appropriate military command authorities. It is important to note that this exception **does not require** covered entities to disclose PHI to commanders, it **only permits** the disclosure. If disclosure is made, then only the minimum amount of information necessary should be provided. Further, the Exception **does not permit** a Commander's direct access to a Service member's electronic medical record, unless otherwise authorized by the Service member or the HIPAA Privacy Rule.

Appropriate military command authorities include commanders who exercise authority over a Service member, or another person designated by a commander.

Authorized activities for which PHI may be disclosed to a commander include but are not limited to:

- Determining the member's fitness for duty;
- Fitness to perform a particular assignment; or
- Carrying out any other activity essential for the military mission.

Mental Health and/or Substance Misuse

To dispel stigma around Service members seeking mental health care or voluntary substance misuse education, DoDI 6490.08 was issued to balance patient confidentiality rights with the commander's need to make informed operational and risk management decisions.

DoD healthcare providers shall **not** notify a Service member's commander when the member obtains mental health care and/or substance misuse education services – **unless** one of the below conditions or circumstances apply. If they apply, then disclosure is required.

- Harm to self. There is a serious risk of self-harm by the member.
- Harm to others. There is a serious risk of harm to others. This includes any disclosures concerning child abuse or domestic violence.
- Harm to mission. There is a serious risk of harm to a specific military mission.
- Special personnel. The member is in the Personnel Reliability Program or has mission responsibilities of such potential sensitivity or urgency that normal notification standards would significantly risk mission accomplishment.
- Inpatient care. The member is admitted or discharged from any inpatient mental health or substance misuse treatment facility.
- Acute medical conditions interfering with duty. The member is experiencing an acute mental health condition or is engaged in an acute medical treatment regimen that impairs the member's ability to perform assigned duties.
- Substance misuse treatment program. The member has entered into, or is being discharged from, a formal outpatient or inpatient treatment program for the treatment of substance misuse.
- Command-directed mental health evaluation. The mental health services are obtained as a result of a command-directed mental health evaluation.
- Other special circumstances. The notification is based on other special circumstances in which proper execution of the military mission outweighs the interests served by avoiding notification, as determined on a case-by-case basis by a covered entity.

If one of these circumstances or conditions applies, DoDI 6490.08 makes the disclosure to the commander permitted AND required.

Substance Misuse Records

Covered entities shall follow the special rules in 42 CFR Part 2 regarding confidentiality of substance misuse patient records.

Privacy Act of 1974

Commanders or other authorized officials receiving PHI from a covered entity shall protect the information in accordance with the Privacy Act to ensure it is only provided to personnel with an official need to know.

Reference:

45 CFR 164.512(k)(1) (Military Command Exception provision of the HIPAA Privacy Rule)

DoD Manual 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019, paragraph 4.4.k (or corresponding provision in successor issuance)

Federal Register Notice, Volume 68, Page 17357, "DoD Health Information Privacy Program," April 9, 2003

DoD Instruction 6490.08, "Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members," August 17, 2011

DoD Directive 6490.02E, "Comprehensive Health Surveillance," August 28, 2017

42 CFR Part 2

DHA "Military Command Exception" webpage at: http://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/HIPAA-Compliance-within-the-MHS/Military-Command-Exception

If you have any questions about any of the information above, please contact the DHA Privacy Office at:
dha.ncr.admin-mgt.mbx.dha-privacyguidance@mail.mil

TMA Privacy and Civil Liberties Office Information Paper

USES AND DISCLOSURES OF PHI FOR LAW ENFORCEMENT PURPOSES

HIPAA Privacy ◆ February 2011

I. Supporting Policies for this Information Paper

A. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 CFR 164.512(f)) sets for the requirements for uses and disclosures of protected health information (PHI) for law enforcement purposes.

B. The Department of Defense Health Information Privacy Regulation (DoD 6025.18-R, C7.6) implements the above section of the HIPAA Privacy Rule as it relates to the Military Health System (MHS).

II. Definitions Associated with Uses and Disclosures of PHI for Law Enforcement Purposes

A. Covered Entity: A health plan or a healthcare provider within the MHS that transmits any health information in electronic form to carry out financial or administrative activities related to healthcare.

B. Disclosure: The release, transfer, provision of access to, or divulging in any other manner of PHI outside the entity holding the information.

C. 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 investigate or conduct an official inquiry into a potential violation of law; or prosecute or conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

D. Military Health System (MHS): All DoD health plans and all DoD healthcare providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by TMA, the Army, the Navy, or the Air Force.

E. Protected Health Information (PHI): Information that is created or received by a covered entity and relates to the past, present, or future physical or mental health of an individual; providing payment for healthcare to an individual; and can be used to identify the individual. It excludes health information in employment records held by a covered entity in its role as employer.

F. Use: With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

III. Guidance Regarding Uses and Disclosures of PHI for Law Enforcement Purposes

A. Minimum Necessary. Except when required by law, PHI disclosures to law enforcement officials should be kept to the minimum necessary as determined by the covered entity. When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official as to what information is the minimum necessary for their lawful purpose.

B. PHI may be disclosed to a law enforcement official to report certain wounds - such as gunshot, stab wounds or other violent injuries - or other physical injuries, as required by law.

1. See Paragraph D.3 for requirements associated with wounds or injuries believed to be the result of abuse, neglect or domestic violence (including child abuse/neglect).

C. PHI may also be disclosed to comply with the requirements of:

1. A court order or court-ordered warrant, or a subpoena or summons is sued by a judicial officer;
2. A grand jury subpoena; or
3. An administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process authorized under law, if the request includes or is accompanied by a written statement verifying the following criteria are met:
    a. The information sought is relevant to a legitimate law enforcement inquiry;
    b. The request is in writing, specific, and limited to the purpose for which the information is sought; and
    c. The information could not reasonably be de-identified.

D. Limiting PHI Disclosures for Identification and Location Purposes.

1. Only the following PHI may be disclosed to law enforcement officials to identify or locate a suspect, fugitive, material witness, or missing person:
    a. Name and address,
    b. Date and place of birth,
    c. Social security number,
    d. ABO blood type and Rh factor,
    e. Type of injury,
    f. Date and time of treatment,
    g. Date and time of death, if applicable; and
    h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

2. Unless otherwise permitted, a covered entity may not disclose any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue to identify or locate an individual.

E. Victims of a Crime.

1. A covered entity may disclose PHI about an individual who is or is suspected to be a victim of a crime if the individual authorizes the disclosure.
2. The covered entity may also disclose PHI in an emergency or if the individual is incapacitated and, therefore, unable to provide authorization, if:
    a. It is shown that the information is needed to determine whether there has been a violation of law by a person other than the victim, and the information is not intended to be used against the victim;
    b. It is shown that immediate law enforcement activity that depends upon the disclosure would be negatively affected by waiting until the individual is able to agree to the disclosure; and
    c. The disclosure is in the best interest of the individual as determined by the covered entity, in the exercise of professional judgment.
3. In cases of adult abuse, neglect or domestic violence and child abuse/neglect:
    a. Adults. A covered entity may disclose PHI related to an adult victim of abuse, neglect, or domestic violence to a government authority that is authorized by law to receive reports of such information if:
        i. The individual agrees to the disclosure; or
        ii. The disclosure is legally required or authorized by law and is compliant with the law, and, in the covered entity's professional judgment, the disclosure is necessary to prevent serious harm to the individual or other potential victims.
    b. Children. A covered entity may disclose PHI related to child abuse or neglect to a government authority that is authorized by law to receive reports of such information without consent from the individual.

F. Decedents. A covered entity may disclose PHI about a decedent to alert law enforcement of the individual's death if there is any suspicion the death may have resulted from criminal conduct.

G. Crime Committed on Covered Entity's Premises. A covered entity may disclose PHI it believes in good faith constitutes evidence of criminal conduct that occurred on the covered entity's premises.

H. Crime Committed off Covered Entity's Premises. A covered healthcare provider furnishing emergency health care on a location other than the covered entity's premises may disclose PHI if the disclosure appears necessary to alert law enforcement to:

1. The commission and nature of the crime;
2. The location of the crime or of the victim(s); and
3. The identity, description, and location of the perpetrator of the crime.

TMA Privacy and Civil Liberties Office Information Paper

THE MINIMUM NECESSARY RULE

HIPAA Privacy ◆ January 2012

I. Supporting Policies for the Minimum Necessary Rule

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 CFR 164.514(d)(1)) establishes the requirements for limiting the use, disclosure and request of protected health information (PHI) by covered entities to the minimum necessary.

B. The Department of Defense Health Information Privacy Regulation (DoD 6025.18-R, C8.2) implements this part of the HIPAA Privacy Rule within the Military Health System (MHS).

II. Definitions Associated with the Minimum Necessary Rule

A. Covered Entity: A health plan or a healthcare provider within the MHS that transmits any health information in electronic form to carry out financial or administrative activities related to healthcare.

B. Disclosure: The release, transfer, provision of access to, or revealing in any other manner of PHI outside the entity holding the information.

C. Military Health System (MHS): All DoD health plans and all DoD healthcare providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by TMA, the Army, the Navy, or the Air Force.

D. Minimum Necessary: The minimum amount of PHI that is reasonably needed to achieve the purpose of a requested use, disclosure or request for PHI.

E. Protected Health Information (PHI): Information that is created or received by a covered entity and related to the past, present, or future physical or mental health of an individual; providing payments for healthcare to an individual; and can be used to identify the individual. It excludes health information in employment records held by a covered entity in its role as employer.

F. Use: With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

III. Guidance for the Minimum Necessary Rule

A. A covered entity must make reasonable efforts to limit the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose of use, disclosure, or request.

B. This does not apply to:

1. Disclosures to or requests by a healthcare provider for treatment.
2. Disclosures to the Secretary of Health & Human Services.
3. Uses and disclosures for purposes of a medical training program.
4. Uses or disclosures to the individual.
5. Uses or disclosures authorized by the individual or a personal representative.
6. Uses or disclosures required by law.

C. Minimum Necessary Uses, Disclosures and Requests of PHI for Non-Treatment Purposes.

1. For routine disclosures and requests, a covered entity should establish policies and procedures that limit the PHI disclosed and requested to the amount reasonably necessary.
2. For non-routine disclosures and requests, a covered entity should:
    a. Develop criteria to limit the PHI disclosed and requested to the amount reasonably necessary, and
    b. Review each disclosure and request individually in accordance with such criteria.

D. Reasonable Reliance. Under certain circumstances, a covered entity may reasonably infer that a requested disclosure is to the minimum necessary when the request is made by:

1. A public official or agency for a disclosure permitted under paragraph C7.4 of DoD 6025.18-R (45 CFR 164.512(d)).
2. Another covered entity.
3. A workforce member or business associate of the covered entity for the purpose of providing professional services to the covered entity; or,
4. An individual requesting the information for research purposes and who provides proper documentation that complies with the applicable requirements.