TO: Local District Commissioners, Medicaid Directors

FROM: Betty Rice, Director
Division of Consumer & Local District Relations

SUBJECT: Chapter 442 of the Laws 2005 Breach of Information Security

EFFECTIVE DATE: December 7, 2005

CONTACT PERSON: James F. Botta Privacy Coordinator
Office of Medicaid Management
518 473 4848

Chapter 442 of the Laws of 2005 entitled the "Information Security Breach and Notification Act" amends the State Technology Law section 208. These provisions require all Local District Medicaid Offices to notify recipients, applicants and respective governmental offices (Attorney General, Consumer Protection Board and the Office of Cyber Security & Critical Infrastructure Coordination) of the unauthorized acquisition of private information which resulted from a breach of information security. The Local District of Social Services (LDSS) enacts policies to perform the required action described below. Penalties are established for failure to notify recipients and applicants and respective government offices

The law was enacted on August 9, 2005 and has an effective date of December 7, 2005

REQUIRED ACTION:

State and local district Medicaid offices maintain Medicaid Confidential Information (MCI) on Medicaid recipients and applicants. This includes all personal enrollment information, financial information, social security number, Medicaid recipient identification number and other confidential information. Both Medicaid regulation(s) and HIPAA regulation(s) require that this information be kept secure and released only for purposes directly related to the administration of the Medicaid program.

All staff must be informed by written notice to staff regarding their responsibility to report suspected breaches of private confidential information to their supervisors or program directors.

The LDSS must have written directives that inform staff about the importance of reporting a breach and how to report such a breach and to whom it must be reported. The LDSS must have a privacy/security officer to whom the LDSS staff will report a suspected privacy breach. The LDSS staff person designated as the HIPAA Officer can also serve in the role of Privacy/Security Officer. The suspected breach must be investigated by the officer and recorded in a log if the breach is confirmed to be in violation of HIPAA and Medicaid confidentiality protections. The log should also record all suspected but not confirmed breaches of security. The breach must be reported to the LDSS Legal Counsel, the Commissioner, the Medicaid Director and the HIPAA officer of the LDSS affected program. If the breach is confirmed, the LDSS Commissioner should authorize written notification to

each person whose information has been illegally disclosed without unreasonable delay as required by law. This notification must be made expeditiously, unless notification impedes a criminal investigation. Notification must be provided, except when notice costs over $ 250,000 or over 500,000 persons are to be notified or insufficient contact information exists. In such cases, posting, alerting local media and e-mailing to and applicants (to the extent possible) must occur.

The Commissioner of the LDSS must also notify the State Attorney General, the Office of Cyber Security and Critical Infrastructure Coordination and the Consumer Protection Board of such breaches. If the information of 5000 or more applicants and/or recipients is breached, consumer reporting agencies (e.g. Equifax) must be notified of the breach.

Local District offices should notify Mr. James F. Botta as to who are the LDSS HIPAA Officer(s). Mr. Botta can be reached via email at jfb04@health.state.ny.us, or by phone at 518-473-4848.

Other important contact information:

State Attorney General
Executive Offices

Albany
The Capitol
Albany, NY 12224-0341
(518) 474-7330

New York City
120 Broadway
New York City, NY 10271
(212) 416-8000

Regional Offices:

Binghamton
44 Hawley Street, 17th Floor
Binghamton, NY 13901-4433
(607) 721-8778

Brooklyn
55 Hansen Place
Brooklyn, NY 11217-1523
(718) 722-3949

Buffalo
Statler Towers
107 Delaware Avenue
Buffalo, NY 14202-3473
(716) 853-8400

Hauppauge
300 Motor Parkway
Hauppauge, NY 11788-5127
(631) 231-1400

Harlem
163 West 125th Street
New York, NY 10027-8201
(212) 961-4475

Mineola
200 Old Country Road
Mineola, NY 11501-4241
(516) 248-3302

Plattsburgh
70 Clinton Street
Plattsburgh, NY 12901-2818
(518) 562-3282

Poughkeepsie
235 Main Street, 3rd Floor
Poughkeepsie, NY 12601-3194
(845) 485-3900

Rochester
144 Exchange Boulevard
Rochester, NY 14614-2176
(585) 546-7430

Syracuse
615 Erie Blvd. W., Suite 102
Syracuse, NY 13210-2339
(315) 448-4800

Utica
207 Genesee St., Room 504
Utica, NY 13501-2812
(315) 793-2225

Watertown
317 Washington Street
Watertown, NY 13601-3744
(315) 785-2444

White Plains
101 East Post Road
White Plains, NY 10601-5008
(914) 422-8755

New York State Consumer Protection Board
5 Empire State Plaza, Suite 2101
Albany, New York 12223
E-Mail Address: webmaster@consumer.state.ny.us

Consumer Assistance Hotline: Toll-Free 1-800-697-1220
Local 518-474-8583
Fax 518-486-3936

Executive Offices: Albany Office
Phone 518-474-3514
Fax 518-474-2474

New York City Office
Phone 212-459-8850
Fax 212-459-8855

New York State
Office of Cyber Security & Critical Infrastructure Coordination
30 S. Pearl Street
Albany, New York 12207-3425

Phone: 518-474-0865
Fax: 518-402-3799
E-Mail: info@cscic.state.ny.us